



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**CYBER FEDERALISM: DEFINING CYBER'S
JURISDICTIONAL BOUNDARIES**

by

Eric Rosner

December 2017

Thesis Co-Advisors:

Ted Lewis
Erik Dahl

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2017		3. REPORT TYPE AND DATES COVERED Master's thesis
4. TITLE AND SUBTITLE CYBER FEDERALISM: DEFINING CYBER'S JURISDICTIONAL BOUNDARIES			5. FUNDING NUMBERS	
6. AUTHOR(S) Eric Rosner				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) Cybersecurity was once a federal government responsibility because cyber had limited impact on state and local entities, but today's cyber risks to critical infrastructure and public services affect all levels of government. This thesis explores the current state of cybersecurity in the United States and examines what role each level of government—federal, state, and local—should play in protecting against and responding to a significant cyber incident. It evaluates current state and local cyber capabilities and outlines the capabilities these governments must develop to play a larger role in this growing homeland security mission. The research concludes that state and local governments should have an important role in cyber preparedness and cyber incident response, but many of these entities lack the capabilities necessary to play a meaningful role. Furthermore, current policies fail to provide clear jurisdictional boundaries between levels of government. Therefore, this thesis recommends that the nation develop a legal framework to improve jurisdictional boundaries, prioritize cyber investments at the state and local level, and improve cyber education. These steps will strengthen state sovereignty and improve the nation's cyber posture.				
14. SUBJECT TERMS Cyber federalism, homeland security, federalism, cybersecurity, cyber incident response, cybercrime, national preparedness, state and local government, 10th Amendment, law enforcement, emergency management, U.S. Constitution			15. NUMBER OF PAGES 127	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**CYBER FEDERALISM: DEFINING CYBER'S JURISDICTIONAL
BOUNDARIES**

Eric Rosner

Director, Continuity of Operations for Cybersecurity and Communications

Department of Homeland Security

B.A., Arizona State University, 2006

J.D., University of Miami, 2010

M.A., Northwestern University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

NAVAL POSTGRADUATE SCHOOL

December 2017

Approved by:

Ted Lewis, Ph.D.
Thesis Co-Advisor

Erik Dahl, Ph.D.
Thesis Co-Advisor

Erik Dahl, Ph.D.
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cybersecurity was once a federal government responsibility because cyber had limited impact on state and local entities, but today's cyber risks to critical infrastructure and public services affect all levels of government. This thesis explores the current state of cybersecurity in the United States and examines what role each level of government—federal, state, and local—should play in protecting against and responding to a significant cyber incident. It evaluates current state and local cyber capabilities and outlines the capabilities these governments must develop to play a larger role in this growing homeland security mission. The research concludes that state and local governments should have an important role in cyber preparedness and cyber incident response, but many of these entities lack the capabilities necessary to play a meaningful role. Furthermore, current policies fail to provide clear jurisdictional boundaries between levels of government. Therefore, this thesis recommends that the nation develop a legal framework to improve jurisdictional boundaries, prioritize cyber investments at the state and local level, and improve cyber education. These steps will strengthen state sovereignty and improve the nation's cyber posture.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	RESEARCH QUESTION	2
C.	HYPOTHESIS.....	3
D.	LITERATURE REVIEW	3
1.	The Hamiltonian Perspective.....	4
2.	The Jeffersonian Perspective	5
3.	Federalism and Homeland Security	7
4.	Conclusion	10
E.	RESEARCH DESIGN	10
II.	EVOLUTION OF THE CYBER THREAT ENVIRONMENT	13
A.	CYBER INCIDENTS DURING THE EARLY DAYS OF THE INTERNET.....	13
B.	CYBER-ATTACKS ON PRIVATE SECTOR ASSETS	15
C.	CYBER-ATTACKS ON NATIONAL ASSETS	16
D.	CYBER-ATTACKS ON STATE AND LOCAL GOVERNMENT ASSETS	19
E.	FEDERAL PREPAREDNESS POLICIES.....	22
F.	FEDERAL CYBERSECURITY AND CRITICAL INFRASTRUCTURE POLICIES.....	23
G.	POLICY IMPLEMENTATION.....	27
H.	CONCLUSION	29
III.	OVERVIEW OF STATE AND LOCAL CYBER CAPABILITIES.....	31
A.	BARRIERS TO CYBER CAPABILITY BUILDING.....	31
1.	Understanding the Threats and Vulnerabilities.....	32
2.	Inadequate Funding.....	34
3.	Workforce Gaps	36
B.	CURRENT STATE AND LOCAL GOVERNMENT CYBER CAPABILITIES.....	37
1.	Strategy	37
2.	Incident Response	39
3.	Cybercrimes and Law Enforcement	41
4.	Information Sharing	43

5.	Research and Development, Education, and Capacity Building.....	44
6.	Commerce	46
7.	Defense	47
C.	STATE AND LOCAL GOVERNMENT BEST PRACTICES.....	48
D.	CONCLUSION	49
IV.	BUILDING A FRAMEWORK FOR JURISDICTIONAL BOUNDARIES IN CYBER.....	51
A.	LEGAL FRAMEWORKS.....	52
B.	FEDERALISM IN OTHER HOMELAND SECURITY MISSIONS	58
1.	Counterterrorism.....	58
2.	Immigration Enforcement.....	60
3.	Emergency Management.....	61
C.	APPLYING THE CONSTITUTION TO CYBER FEDERALISM.....	63
D.	CONCLUSION	64
V.	RECOMMENDATIONS AND CONCLUSION.....	67
A.	RECOMMENDATION 1: IMPROVE THE LEGAL FRAMEWORKS AND JURISDICTIONAL BOUNDARIES	67
1.	Recommendation 1.1: Clarify Cyber Incident Responsibilities within State and Local Governments	68
2.	Recommendation 1.2: Formalize Cyber Roles and Responsibilities between Levels of Government	69
3.	Recommendation 1.3: Strengthen Cybercrime Prosecution by Standardizing Cyber Laws.....	71
B.	RECOMMENDATION 2: INCREASE CYBER INVESTMENTS AND MAXIMIZE EXISTING RESOURCES.....	75
1.	Recommendation 2.1: Prioritize Cybersecurity in Future Budgets and Create a Federal Cyber Grant Program	76
2.	Recommendation 2.2: Enhance Threat Detection and Indicator Sharing through State-led Cyber Operation Centers and/or by Expanding the Roles and Capabilities of Fusion Centers	77
3.	Recommendation 2.3: Create an Agile Cyber Workforce with the Ability to Expand during a Cyber Incident.....	78
4.	Recommendation 2.4: Create “Cyber 9-1-1” to Centralize Cyber Incident Reporting	79

C.	RECOMMENDATION 3: EMPHASIZE CYBER EDUCATION AND COLLABORATION AMONG THE PUBLIC SECTOR, PRIVATE SECTOR, AND ACADEMIA	80
1.	Recommendation 3.1: Incorporate Cyber Education in School Curriculums for Children of All Ages	80
2.	Recommendation 3.2: Place Greater Emphasis on Computer Science Programs in Universities	81
3.	Recommendation 3.3: Develop Technology Parks that Bring the Public Sector, Private Sector, and Academia to a Central Location	81
D.	CONCLUSION	82
APPENDIX. CYBER INCIDENT SEVERITY SCHEMA		85
LIST OF REFERENCES		87
INITIAL DISTRIBUTION LIST		105

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Proposed Cybercrimes Classifications and Sentencing Guidelines.....	74
Table 2.	Overview of Recommendations.....	83
Table 3.	PPD-41 Cyber Incident Severity Schema.	85

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARPA	Advanced Research Projects Agency
CISO	Chief Information Security Officer
CALEA	Communications Assistance for Law Enforcement Act
CFAA	Computer Fraud and Abuse Act
CDRT	Cyber Disruption Response Team
DHS	Department of Homeland Security
DDOS	distributed denial of service
EO	executive order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HSPG	Homeland Security Preparedness Grant
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ITA	Information Technologies Agency
IBM	International Business Machine
JTTF	Joint Terrorism Task Force
NASCIO	National Association of State Chief Information Officers
NCIRP	National Cyber Incident Response Plan
NGA	National Governors Association
NIMS	National Incident Management System
NIST	National Institute for Standards and Technology
NIIMS	National Interagency Incident Management System
NPR	National Preparedness Report
NJCCIC	New Jersey Cybersecurity and Communications Integration Cell
NIPP	National Infrastructure Protection Plan
OPM	Office of Personnel Management
ODNI	Office of the Director of National Intelligence
PC	personal computer
PII	personally identifiable information
PKEMRA	Post-Katrina Emergency Management Reform Act of 2006

PPD	Presidential Policy Directive
SSA	Sector-Specific Agency
SCADA	supervisory control and data acquisition

EXECUTIVE SUMMARY

As technology matures and produces new opportunities for human advancement, it also creates new threats and vulnerabilities. Today's interconnected and interdependent systems heighten these risks because they increase the likelihood of a cyber-attack having cascading consequences across the country. The federal government plays a large role in cyber preparedness and cyber incident response, but as the frequency and severity of cyber-attacks continue to grow, the nation must decide the proper balance between all levels of government in the cyber mission space. This thesis argues that the nation should address this escalating threat by embracing cyber federalism—a bottom-up approach where state and local governments play a larger role in cybersecurity. Cyber federalism would allow the federal government to focus resources on significant cyber threats, while empowering state and local governments to manage their own cybersecurity needs.

The cyber threat has evolved from a localized problem impacting a small number of computers within isolated systems to a boundless danger for highly interconnected systems. This evolution forced the federal government to develop a range of policies aimed at improving cyber preparedness and cyber incident response. For example, *Presidential Policy Directive (PPD) 41: United States Cyber Incident Coordination* organizes the federal government's cyber response efforts by clarifying the roles and responsibilities of all federal entities with a cyber mission. The federal government also utilizes several information sharing mechanisms—such as Information Sharing and Analysis Centers (ISAC), Information Sharing and Analysis Organizations (ISAO), and fusion centers—to improve collaboration with public and private sector partners. These policies and programs have helped the federal government improve their cyber capabilities, but the current cyber threat environment is too complex for the federal government to handle alone.

In many instances, state and local governments are the first line of defense, especially if the cyber incident affects public services or critical infrastructure. Unfortunately, most state and local governments still struggle to develop the cyber capabilities required to prepare for and respond to these cyber threats. In 2013, the

Potomac Institute for Policy Studies developed the *Cyber Readiness Index*, which evaluates seven elements to gauge an entity's cyber preparedness.¹ These elements are: (1) strategy; (2) incident response; (3) cybercrime and law enforcement; (4) information sharing; (5) research and development, education, and capacity building; (6) commerce; and (7) defense.² This thesis evaluates state and local cyber capabilities by examining their maturity in these seven categories and highlighting best practices from states that have found proficiency in these areas.

This thesis also examines the legal constructs that shape the debate between federalism and a strong central government. For example, the Necessary and Proper Clause grants the federal government significant power to enact laws and the Supremacy Clause prevents states from enforcing any laws that conflict with federal statutes.³ However, these constitutional provisions are counterbalanced by the 10th Amendment, which strengthens state sovereignty by granting states all powers to govern that are not reserved for the federal government.⁴ Together, these principles guide the jurisdictional balancing act among the various levels of government and provide a legal framework for each government's underlying authorities. Tension over authority also exists in several homeland security missions, such as law enforcement and emergency services, because multiple levels of government play a role, but the nation has mitigated this strain by clarifying jurisdictional boundaries. Moving forward, state and local governments can learn from these examples as they examine their role in the cyber mission.

Ultimately, this thesis concludes that the growing cyber threat is too complex and expansive for the federal government to handle alone so state and local governments must develop the cyber capabilities necessary to play a larger role. It recommends three courses of action to strengthen state and local cyber capabilities and to empower these

¹ Melissa Hathaway, *Cyber Readiness Index 2.0*, Potomac Institute for Policy Studies, November 2015, 4, <http://www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-index-2.0-web-2016.pdf>.

² Ibid. Also, note that the *Cyber Readiness Index* identifies “diplomacy and trade” as an element, but this has been renamed to “commerce” in this thesis as it more closely aligns with the responsibilities of state and local governments.

³ U.S. Const. art. I, § 8, and U.S. Const. art. VI, § 2.

⁴ U.S. Const. amend. X.

governments in the cyber mission space. First, the nation should develop a legal framework to improve jurisdictional boundaries across all levels of government. Second, the nation should prioritize cyber investments at the state and local level. Third, state and local governments, in collaboration with the federal government, should improve cyber education at all grade levels. Overall, if the nation wants to maintain its reputation as a world leader in the cyber community and improve its cyber posture, it must embrace a bottom-up approach that gives state and local governments a more significant role in cybersecurity. Cyber federalism would make the nation more adaptable and dynamic when protecting against rapidly evolving cyber threats, which improves the security of the nation as a whole.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I have many people to thank for helping me get through this program and for guiding me through the thesis process, but I must start by thanking my beautiful wife, Alisha, for her love and support. It has been a chaotic 18 months trying to balance work, school and a wedding, but we managed to make it through. I could not have done this without you.

To my parents, thank you for your weekly check-ins and for constantly pushing me to advance my education. To my brother, thanks for putting up with my brotherly advice, even when you do not want it. I hope you can learn from some of my school experiences as you persevere through medical school.

To my former colleagues at FEMA, thank you for nominating me to this program and encouraging me to pursue this unbelievable opportunity. A special thanks to Kawana Cohen-Hopkins, Caitlin McCarthy Clarke, and Fred Dolan for your mentorship and patience. I am forever indebted to you all for everything you taught me throughout my tenure at FEMA.

To my leadership in CS&C, thank you for allowing me to continue the program and for encouraging me to further my education. A special thanks to Dan Medina and Lisa Teetz for remaining patient through my quarterly trips to California, especially when work was chaotic in my absence. I am also grateful for your guidance and for providing me with the knowledge and support to succeed in our important mission.

To my advisors, Ted Lewis and Erik Dahl, I would have never completed this thesis without your insight, support, dedication and expertise. When you both convinced me to switch topics halfway through the program, I did not think I could ever finish this thesis on time, but I did thanks to your incredible responsiveness and your ability to focus me when my thoughts had gone astray. You both always knew how to ask the right questions and make me think harder, even when I thought I had the right answer.

To the faculty of the Naval Postgraduate School and my incredible classmates, thank you for the thought-provoking conversations and for sharing some of your

unbelievable experiences with me. Cohort 1601-1602 is an incredible collection of talent, kindness, and honor. The future of homeland security is bright with these fine men and women leading the way.

I am truly grateful to all of you for everything you all have done. Thank you.

I. INTRODUCTION

Our nation's cybersecurity teeters on the edge of a precipice, struggling to maintain its footing as the ever-increasing barrage of cyber-attacks threatens safety and security. The number of cyber incidents continues to increase each year at an alarming rate, while the growing interconnectivity of digital devices improves the likelihood of significant cyber incidents and intensifies their consequences.¹ A significant cyber incident could cripple the U.S. economy and infrastructure, leaving the nation vulnerable to significant loss of life and causing irreparable damage to essential life functions.² This potential for catastrophic disaster forces the United States to focus enormous resources on building cybersecurity capabilities.³

A. PROBLEM STATEMENT

In 2013, President Obama unveiled *Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity*, which called for a cybersecurity risk management framework and improved incentives for the adoption of cybersecurity best practices.⁴ Three years later, President Obama released *Presidential Policy Directive (PPD) 41: United States Cyber Incident Coordination*, which describes how the federal government's cyber entities coordinate cyber preparedness and incident response efforts.⁵ EO 13636 and PPD-41 are important steps but more work remains.

¹ James Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence, February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

² Ibid.

³ "Fact Sheet: Cybersecurity National Action Plan," White House Archives, February 9, 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

⁴ Barack Obama, "Executive Order – Improving Critical Infrastructure Cybersecurity," White House Archives, February 12, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

⁵ Barack Obama, "Presidential Policy Directive – United States Cyber Incident Coordination," White House Archives, July 26, 2016, <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.

Shortly after PPD-41 was released, government officials found evidence of malicious actors attempting to penetrate election ballot systems during the 2016 presidential election.⁶ The Department of Homeland Security (DHS) responded by designating election infrastructure as critical infrastructure, thereby making it a protection priority within the “National Infrastructure Protection Plan” (NIPP).⁷ This allowed DHS to increase technical assistance to state and local election officials upon request, but many states saw this as an infringement on states’ rights and a step toward a federal takeover of the election process.⁸ The dispute underscored a disconnect between the states and the federal government on the proper level of involvement when state and local governments fall victim to cyber-attacks.

Current cyber policies help clarify federal roles and responsibilities, but there are few policies addressing the proper role that each level of government—federal, state, and local—must play in the cybersecurity mission. Other homeland security missions, like law enforcement and emergency management, have clear roles and responsibilities for each level of government, but cyber’s jurisdictional boundaries are less clear. Therefore, using the principles outlined in PPD-41 and the standards set forth in physical response efforts, the nation can and should develop strategies and operational plans to maximize government capabilities and improve the security and resilience of our digital systems.

B. RESEARCH QUESTION

What role should each level of government—federal, state, and local—play in protecting against and responding to a significant cyber incident?

⁶ Scott Malone, “Russian Election Hacking ‘Wildly Successful’ in Creating Discord: Former U.S. Lawmaker,” Reuters, May 4, 2017, <http://www.reuters.com/article/us-usa-trump-russia-idUSKBN17Y2ON>.

⁷ Jeh Johnson, “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector,” DHS, January 6, 2017, <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.

⁸ Katie Bo Williams, “DHS Designates Election Systems as ‘Critical Infrastructure’,” The Hill, January 6, 2017, <http://thehill.com/policy/national-security/313132-dhs-designates-election-systems-as-critical-infrastructure>.

C. HYPOTHESIS

While the federal government continues to make progress in developing comprehensive cybersecurity policies, these strategies have not kept pace with advancements in technology, leaving the nation vulnerable to potentially catastrophic cyber-attacks. State and local governments are even further behind, thereby forcing them to rely heavily on the federal government for support in cybersecurity. This inefficient cycle exhausts resources and widens the capability gap; therefore, the nation needs a new strategy that enables state and local governments to develop their own capabilities, while also empowering them to utilize these capabilities. The evolving and expanding cyber threat landscape requires an all-of-nation approach to cybersecurity, which means state and local governments should take larger roles in protecting against and responding to cyber incidents.

The objective of this thesis is to develop a strategy that clarifies jurisdictional boundaries between government entities before and during a cyber incident response. It takes a bottom-up approach, examining the current capabilities of state and local governments, and then recommends strategies to clarify responsibilities. It also underscores the importance of cyber federalism and provides a path forward as all levels of government search for their role in the cyber mission.

D. LITERATURE REVIEW

As technological risks continue to mature and increase in severity, there is also a growing body of literature exploring how the United States prepares for and responds to cyber incidents. These risks pose a serious threat to our national security so it is important to create a strategy that develops cyber capabilities and clarifies the roles and responsibilities for all levels of government. Ultimately, such a strategy must explore how federalism influences cyber response efforts.

America has long debated the proper balance of authority between the federal government and the states. In fact, during the drafting of the Constitution several framers worried states would refuse to ratify the document for fear of sacrificing state

sovereignty.⁹ On one side of the debate was Thomas Jefferson, who believed that the states should maintain power or else Americans risked reliving the tyranny they fled in Europe.¹⁰ On the other side was Alexander Hamilton, who believed that a strong central government was critical to the continued development and success of a growing nation.¹¹ The remainder of this literature review assesses the Hamiltonian and Jeffersonian perspectives on federalism and examines this discussion from the homeland security viewpoint.

1. The Hamiltonian Perspective

Perhaps the greatest insight into the minds of the framers of the Constitution comes from “The Federalist Papers,” a series of articles drafted by Alexander Hamilton, James Madison, and John Jay, promoting the principles of the Constitution and encouraging its ratification.¹² “The Federalist Papers” provided Hamilton with a platform to convince the public that a federal government was critical to the security and long-term viability of the newborn nation.¹³

In *Federalist Paper 9: The Union as a Safeguard against Domestic Faction and Insurrection*, Hamilton addressed the public’s anti-federalist angst by explaining that the United States would be different than the English monarchy structure because the United States was a confederated system that focused on cooperation between states, not strong federal oversight.¹⁴ Essentially, he argued that the federal government was designed to protect the interests of each state, not undermine or override state governments.

⁹ “The Constitution,” White House: Our Government, accessed November 4, 2017, <https://www.whitehouse.gov/1600/constitution>.

¹⁰ Merrill D. Peterson, ed., *A Summary View of the Rights of British America*, Thomas Jefferson: Writings, New York: The Library of America, 1984, p. 118.

¹¹ James Madison, “Federalist Number 10,” Congressional Resources, 1787, <https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-10>.

¹² “About the Federalist Papers,” Congressional Resources, accessed November 4, 2017, <https://www.congress.gov/resources/display/content/About+the+Federalist+Papers>.

¹³ Ibid.

¹⁴ Alexander Hamilton, “Federalist Number 9,” Congressional Resources, 1787, <https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-9>.

In *Federalist Paper 10: The Same Subject Continued: The Union as a Safeguard against Domestic Faction and Insurrection*, Madison and Hamilton concurred with Scottish philosopher David Hume's theory that large democracies are less vulnerable to tyranny from over-ambitious majorities because there are more checks and balances in place to protect the greater good.¹⁵ Hamilton reemphasized the value of checks and balances through a large democracy in *Federalist Paper 67: The Executive Department*, where he highlighted the rules that limit executive branch authority.¹⁶ He argued that the Constitution provided several checks and balances within the federal government to ensure that no one branch of government could seize control of the nation or maintain undue influence.¹⁷

2. The Jeffersonian Perspective

While Thomas Jefferson once described "The Federalist Papers" as the "best commentary on the principles of government which ever was written," he did not necessarily agree with all of the arguments outlined in the 85 articles.¹⁸ In 1774, Jefferson penned *A Summary View of the Rights of British America*, which cautioned against an overzealous and unrestrained government because inadequate checks and balances led to tyranny.¹⁹ He understood the importance of a federal government, even serving as the third President of the United States, but remains one of the most important supporters of states' rights in United States history.²⁰

Several of the Founding Fathers concurred with the Jeffersonian view on governing and disagreed with the beliefs outlined in "The Federalist Papers," which led

¹⁵ Madison, "Federalist Number 10."

¹⁶ Alexander Hamilton, "Federalist Number 67," Congressional Resources, 1787, <https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-67>.

¹⁷ Ibid.

¹⁸ "Thomas Jefferson: Establishing a Federal Republic," Library of Congress, accessed November 4, 2017, <https://www.loc.gov/exhibits/jefferson/jefffed.html>.

¹⁹ Peterson, *A Summary View of the Rights of British America*, p. 118.

²⁰ "Thomas Jefferson," White House, accessed November 4, 2017, <https://www.whitehouse.gov/1600/presidents/thomasjefferson>.

to a series of response papers known as “The Anti-Federalist Papers.”²¹ While these did not have the same lasting impact enjoyed by “The Federalist Papers,” they gave the countermovement a voice and reinforced the importance of states’ rights. For example, in *Anti-Federalist Paper 45: Powers of National Government Dangerous to State Governments; New York as an Example*, Robert Yates warned that the proposed Constitution made states subordinate to the federal government, “existing solely by its toleration, and possessing powers of which they may be deprived whenever the general government is disposed so to do.”²² He worried that the 10th Amendment, which asserts “the powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people,” did not provide adequate protection for state sovereignty.²³

However, Yates failed to account for other protections, such as the judicial branch, which allows savvy states to influence federal government policies even when they lack the legal authority to direct federal actions. In *Arming States’ Rights: Federalism, Private Lawmakers, and the Battering Ram Strategy*, Barak Orbach, Kathleen Callahan, and Lisa Lindemenn argue that states can influence federal policies by challenging them in court.²⁴ Even when states do not win these cases, the mere challenge may put enough political pressure on the federal government to revise unpopular policies.²⁵ The authors contend that “uncooperative federalism,” which is a “set of strategies that uses states’ regulatory powers to challenge the federal government,” allows states to exercise power over federal policymaking, even when armed with limited legal authority.²⁶

²¹ “Anti-Federalist Papers,” The Federalist Papers Project, accessed November 4, 2017, <http://thefederalistpapers.org/anti-federalist-papers>.

²² Robert Yates, “Antifederalist Paper 45,” The Federalist Papers Project, accessed November 4, 2017, <http://thefederalistpapers.org/antifederalist-paper-45>.

²³ U.S. Const. amend. X.

²⁴ Barak Orbach, Kathleen S. Callahan, and Lisa M. Lindemenn, “Arming States’ Rights: Federalism, Private Lawmakers, and the Battering Ram Strategy,” *Arizona Law Review*, Vol 52, November 15, 2010, <https://ssrn.com/abstract=1696012>.

²⁵ Ibid.

²⁶ Ibid. at 1163.

Overall, the spirited debates between the Hamiltonians and the Jeffersonians shaped today's multilayered governing system that provides centralized leadership, while still providing mechanisms for the states to retain their sovereignty and assert their authority. As the country expanded in size and complexity, so did the scope of the federalism conversation; therefore, the next section focuses on the current literature that guides today's dialogue, as it relates to the role of federalism in homeland security issues.

3. Federalism and Homeland Security

Homeland security is no stranger to the federalism debate. When Congress created DHS in 2003, it was the largest reorganization of federal agencies with a homeland security focus since the National Security Act of 1947.²⁷ As a result, it created new jurisdictional overlap within the federal government but also between federal entities and their state counterparts.²⁸ In *Federalism and Homeland Security: Our Constitutional System of Governance*, Nadav Morag outlines the power struggle between public safety organizations from all levels of government.²⁹ Morag argues, "The time-honored debate over federal vs. state and local power is very much alive in the homeland security realm," and existing turf wars have expanded as the homeland security mission broadens.³⁰ In other words, jurisdictional lines continue to blur as the homeland security mission evolves.

Other scholars point out that the Hamilton versus Jefferson-style debate on the proper role of each level of government is further complicated in catastrophic events. For example, In *Federalism, Law Enforcement, and the Supremacy Clause: The Strange Case of Ruby Ridge*, Seth Waxman of the Georgetown University Law Center outlines the "anti-commandeering" principle, which prevents the federal government from demanding that state and local authorities assist in enforcing federal laws, even during an event of

²⁷ *National Security Act*, 50 U.S.C. 15 (1947) § 401.

²⁸ Nadav Morag, "Federalism and Homeland Security: Our Constitutional System of Governance," Colorado Technical University, September 10, 2012, <http://www.coloradotech.edu/resources/blogs/september-2012/federalism-and-homeland-security>.

²⁹ *Ibid.*

³⁰ *Ibid.*

national significance.³¹ The principle ensures the autonomy of the states, even during a crisis, but it is unclear if this principle would withstand the test of a national emergency.³² Specifically, Waxman notes that the Supreme Court created the “anti-commandeering” principle before the terrorist attacks on September 11, 2001, and reasons that the public may have a higher tolerance for, or even expect, federal intervention in a post-9/11 era.³³

Conversely, in *Reflections on Homeland Security and American Federalism*, scholar Pietro S. Nivola argues that most homeland security issues are local and should be handled by local authorities.³⁴ Like Jefferson, he concedes that the federal government plays an important role, but believes the federal government should focus its resources on inherently federal functions, like border security and preventing international terrorism.³⁵ Interestingly, Nivola does not mention whether he views cybersecurity as a state or federal issue.³⁶ Similarly, in *Learning from Disaster: The Role of Federalism and the Importance of Grassroots Response*, authors James Carafano and Richard Weitz contend that “Homeland security and disaster management are national, not just federal, missions.”³⁷ While the federal government can support responders by facilitating information sharing across jurisdictions and providing the resources required for an effective response, the states are best positioned to lead emergency response efforts.³⁸

³¹ Seth P. Waxman, “Federalism, Law Enforcement, and the Supremacy Clause: The Strange Case of Ruby Ridge,” *Georgetown Law Faculty Publications*, March 2010, <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1279&context=facpub>.

³² Ibid.

³³ Ibid. at 153.

³⁴ Pietro S. Nivola, “Reflections on Homeland Security and American Federalism,” Brookings Institute, May 13, 2002, <https://www.brookings.edu/articles/reflections-on-homeland-security-and-american-federalism/>.

³⁵ Ibid.

³⁶ Ibid.

³⁷ James Carafano and Richard Weitz, “Learning from Disaster: The Role of Federalism and the Importance of Grassroots Response,” The Heritage Foundation, March 21, 2006, <http://www.heritage.org/homeland-security/report/learning-disaster-the-role-federalism-and-the-importance-grassroots>.

³⁸ Ibid.

The literature also acknowledges that the transnational nature of cyber threats requires a coordinated effort from all levels of government. For example, in *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, Kristin M. Finklea argues that cybersecurity not only blurs jurisdictional boundaries in the United States, it also causes jurisdictional confusion on an international scale.³⁹ As a result, the cyber threat is simply too tangled and complex for the federal government to handle alone.⁴⁰ Instead, federal entities have used interagency agreements and memoranda of understandings to outline authorities on a case-by-case basis.⁴¹ This has led to improved information sharing and coordination, which minimizes the burden on state and local resources.⁴²

In *State-Level Cybersecurity*, Michael Glennon goes one step further by suggesting that states must take more responsibility in cybersecurity because the federal government and the international community have “largely dropped the ball.”⁴³ Glennon asserts that the federal government has the technology to protect networks, sharing threat indicators, and mitigate the consequences of attacks, but the technology has not been implemented effectively; therefore, it is up to the states to take responsibility for their own security.⁴⁴ He also argues that states should invest resources to become self-sufficient in cybersecurity because these cyber defense capabilities can lead to long-term financial benefits.⁴⁵

Overall, the literature contends that as states and local governments continue to become more reliant on technology to provide public services and support their citizens, the need to protect these complex systems becomes increasingly a state and local issue.

³⁹ Kristin M. Finklea, “The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement,” Congressional Research Service, January 17, 2013, <https://fas.org/sgp/crs/misc/R41927.pdf>.

⁴⁰ Ibid.

⁴¹ Ibid.

⁴² Ibid.

⁴³ Michael J. Glennon, “State-Level Cybersecurity,” Hoover Institute at Stanford University, February 1, 2012, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997565.

⁴⁴ Ibid.

⁴⁵ Ibid.

While the federal government and state governments have clearly defined roles in law enforcement and emergency management efforts, cyber authorities are less clear; therefore, the nation must help states develop their cyber capabilities and improve the nation's cybersecurity posture as a whole.

4. Conclusion

In conclusion, there is a significant body of literature analyzing the proper role of the federal government in governing the nation, but neither side has found the perfect balance between levels of government in a democracy. Even visionaries like Alexander Hamilton and Thomas Jefferson could not predict the technological advancements of society and how these advancements alter the relationship between the federal government and the states. The remainder of this thesis explores this dynamic and evaluates the proper balance between the federal government and state governments in cybersecurity. Ultimately, it sides with the Jeffersonian perspective that state and local governments must play a larger role in cybersecurity. Therefore, the nation must empower states in the cyber mission space by clarifying jurisdictional boundaries and providing them with the resources necessary to develop and sustain their own cyber capabilities.

E. RESEARCH DESIGN

This thesis focuses on policy considerations for cybersecurity in the public sector, but does not tackle the technical aspects of cybersecurity or critique tactics, techniques, or procedures used to combat cyber threats or gather information on cyber threats. Furthermore, while much of cybersecurity operates in a classified setting, the research in this thesis focuses solely on open-source materials and is meant for the widest possible distribution. It also focuses on public sector cybersecurity, not on the private sector.

Information for this thesis comes from primary and secondary sources that cover federalism and national security issues—such as national preparedness, critical infrastructure protection, and cybersecurity. Primary sources include statutes, court decisions, testimony from legislative hearings, and unclassified documents from the

executive branch. These documents provide insight into current cyber incident response policies, including organizational roles and responsibilities.

The secondary resources include newspaper articles, magazine articles, and books that discuss cybersecurity, cyber incident response, and related national security items. These documents provide an overview of the public discussion on cyber issues for government entities and highlight key opinions in this field. These sources also offer context to the primary sources and incorporate analysis on relevant policies in homeland security.

This thesis employs a policy options analysis because current cyber incident response policies do not address jurisdictional conflicts in homeland security. The first step in this analysis process is to define the problem—that there is insufficient guidance on the division of labor between levels of government during a cyber incident. Therefore, this thesis examines existing federal cybersecurity policies, surveys state and local cyber policies, and identifies ways to bridge policy gaps between each level of government by articulating a framework for jurisdiction clarification. While there is no magic solution that prevents all cyber threats or perfects cyber incident response, a complete analysis provides solutions to improve cyber preparedness at the state and local level.

The criteria for judging final recommendations is a jurisdiction's ability to implement the policy within existing resource constraints and the likelihood the implemented policy will improve the nation's ability to respond to a cyber incident. While the second measure can be broadly defined, for the purposes of this thesis, it will be measured by the likelihood state and local governments understand their role and their ability to fulfill their responsibilities. These recommendations must account for resource constraints, the disparities in capabilities between states and between jurisdictions within each state, and the potential consequences of implementation.

The final output is a set of recommendations that outline a strategy for enhancing state and local government cyber capabilities and a jurisdictional framework that clarifies how government organizations utilize these capabilities during cyber incidents. The document aims to clarify jurisdictional ambiguities and strengthen capability gaps so

government entities are able to respond to incidents within their purview. This discussion will provide a foundation for policymakers to organize response efforts and maximize resources. This thesis begins by describing the evolution of cyber threats and outlining the federal cyber policies and programs. It then examines the current cyber capabilities of state and local governments, outlines how to define jurisdictional boundaries for each level of government, and recommends strategies for how state and local governments can improve their capabilities to meet these target responsibilities.

II. EVOLUTION OF THE CYBER THREAT ENVIRONMENT

In the 1960s, computers were massive machines that cost millions of dollars, with minimal processing power and limited ability to communicate with other machines.⁴⁶ This dynamic changed forever when International Business Machines (IBM) released the first mass-produced personal computer (PC) and the Department of Defense's (DOD) Advanced Research Projects Agency (ARPA) developed ARPANET, the precursor to the Internet.⁴⁷ Together, the personal computer and the Internet unlocked limitless possibilities for the future of digital technology, but also dramatically increased system vulnerabilities. This chapter examines some of the most significant cyber incidents since the advent of the Internet, highlights trends in a rapidly evolving cyber threat environment, and explains how significant cyber incidents shape current national cybersecurity policies and programs.

A. CYBER INCIDENTS DURING THE EARLY DAYS OF THE INTERNET

In 1988, with the Internet still in its infancy, Robert Morris, Jr. developed the *Morris* worm, which was one of the first examples of widespread computer malware in history.⁴⁸ A worm is software that travels from computer to computer on its own.⁴⁹ This differs from a virus, which is software that travels from computer to computer with the assistance of an intermediary, such as a human user.⁵⁰ Worms and viruses are both forms of malware, which is any software designed to gain unauthorized access to a computer and do harm.⁵¹ The *Morris* worm infected roughly 6,000 machines, or roughly 10 percent

⁴⁶ "Timeline of Computer History," Computer History Museum, accessed November 4, 2017, <http://www.computerhistory.org/timeline/1961/>.

⁴⁷ "Birth of the Internet," PBS, accessed November 4, 2017, <http://www.pbs.org/transistor/background1/events/arpnet.html>.

⁴⁸ "Cyber Timeline," NATO Review Magazine, accessed November 4, 2017, <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>.

⁴⁹ "What Is the Difference: Viruses, Worms, Trojans, and Bots," Cisco, accessed November 4, 2017, <http://www.cisco.com/c/en/us/about/security-center/virus-differences.html>.

⁵⁰ Ibid.

⁵¹ Ibid.

of the Internet users at the time.⁵² Morris was later the first person convicted under the Computer Fraud and Abuse Act (CFAA), which solidified the CFAA as a tool for protecting the integrity of digital systems.⁵³ However, the cyber-attack was also a wake-up call to the general public on the power of the Internet and demonstrated that the CFAA alone would not prevent further cyber incidents.

Right before the turn of the century, in 1999, the *Melissa* virus became the first virus to use email for mass transmittal and became the fastest spreading virus of all time.⁵⁴ The virus would access the infected user's email contacts list and send an email with the virus to every single email address in that list.⁵⁵ While the *Melissa* virus did not cause damage by deleting or stealing files, it did wreak havoc on the Internet by shutting down email systems for several days.⁵⁶ A year later, the *I Love You* virus used the same method to infect roughly 45 million Windows PC users.⁵⁷

The damage caused by the *Melissa* virus and the *I Love You* virus highlighted the Internet's rapid expansion and demonstrated the growing risks of the digital world. In 1988, the United States government panicked when the *Morris* worm infected roughly 6,000 users, but 11 years later malware was capable of infecting over 7,000 times as many users in days. The next section illustrates how these early malware infections were only the beginning. As technology matured in the 21st century, malicious actors continued to develop their cyber capabilities and found new ways to use these skills to attack assets throughout the world.

⁵² Cara Giaimo, "In 1988, One Rogue Worm Shut Down 10 Percent of the Internet," Atlas Obscura, November 3, 2015, <http://www.atlasobscura.com/articles/in-1988-one-rogue-worm-shut-down-10-percent-of-the-internet>.

⁵³ "Headliners: Accessing Jail?" New York Times, January 28, 1990, <http://www.nytimes.com/1990/01/28/weekinreview/headliners-accessing-jail.html>.

⁵⁴ Elinor Mills, "Melissa Virus Turns 10," CNET, March 31, 2009, <https://www.cnet.com/news/melissa-virus-turns-10/>.

⁵⁵ David Kleinbard and Richard Richtmyer, "U.S. Catches 'Love' Virus," May 5, 2000, <http://money.cnn.com/2000/05/05/technology/loveyou/>.

⁵⁶ "IDFAQ: What was the Melissa Virus and what can We Learn from it?" SANS Institute, accessed November 4, 2017, <https://www.sans.org/security-resources/idfaq/what-was-the-melissa-virus-and-what-can-we-learn-from-it/5/3>.

⁵⁷ Mark Ward, "A Decade on from the ILOVEYOU Bug," BBC, May 4, 2010, <http://www.bbc.com/news/10095957>.

B. CYBER-ATTACKS ON PRIVATE SECTOR ASSETS

While hackers were able to cause chaos and gain notoriety in the 20th century, by the early stages of the 21st century malicious actors were able to monetize their infiltrations by stealing treasure troves of data from large international corporations.⁵⁸ For example, from 2003 to 2004 the TJX Companies Incorporated—which owns well-known discount stores like TJ Maxx and Marshalls—was victimized by a group of hackers that uncovered vulnerabilities in the company’s wireless credit card services and data storage systems.⁵⁹ The perpetrators stole data from roughly 45.7 million customers, causing over \$250 million in damage.⁶⁰ It also set the stage for other large-scale cyber-attacks to mega corporations, such as the Heartland Payment Systems (2008), Epsilon (2011), and Target (2013).⁶¹

Some prominent cyber-attacks on the private sector are state-sponsored initiatives designed to gather information through cyberespionage. For example, in 2010, Google announced that it was a victim of a highly sophisticated and targeted attack by hackers with ties to the Chinese government.⁶² The attack, coined Operation Aurora, aimed to monitor Chinese human rights activists by penetrating their computer systems through their Google email accounts.⁶³ While Google was able to mitigate the damage of this attack by acting quickly and publicizing China’s malfeasance, China and other nation-state actors continue to find new ways to breach private sector systems for invaluable customer data. This trend is likely to continue as companies improve their ability to track

⁵⁸ Evan Schuman, *The TJX Data Loss and Security Breach Case*, University of Sydney: Engineering and Information Technology, 2007, http://sydney.edu.au/engineering/it/courses/info5990/Supplements/Week07_Malware&Security/Supp07-4TJXCaseDetails.pdf.

⁵⁹ Ibid.

⁶⁰ “10 Most Costly Cyber Attacks in History,” Business Pundit, August 15, 2011, <http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history/>.

⁶¹ Mary Helen Miller, “Data Theft: Top 5 Most Expensive Data Breaches,” The Christian Science Monitor, May 4, 2011, <http://www.csmonitor.com/Business/2011/0504/Data-theft-Top-5-most-expensive-data-breaches/3.-TJX-256-million-or-more>.

⁶² David Drummond, “New Approach to China,” Google Official Blog, January 12, 2010, <https://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.

⁶³ Ariana Eunjung Cha and Ellen Nakashima, “Google China Cyberattack Part of a Vast Espionage Campaign, Experts Say,” Washington Post, January 14, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html>.

consumer habits and predict consumer behavior because nation-states can use the same information to spy on large populations.

The 2013 and 2014 data breaches of Yahoo's user account data are also examples of large-scale attacks by a nation-state.⁶⁴ Experts believe the Russian government orchestrated two large-scale cyber-attacks on Yahoo to collect user account data and acquire access to user records and emails.⁶⁵ Yahoo estimates that the malicious actors stole data on three-billion users, but the true costs remain unclear as it is impossible to know how these hackers used this data and what other systems they breached through the sensitive information they collected.⁶⁶

As Russian hackers were infiltrating Yahoo's massive databases, North Korean forces penetrated Sony Pictures' systems, stole employees' personally identifiable information (PII) and emails, and posted this information on the Internet.⁶⁷ The incident embarrassed the company and left employees' private information vulnerable to mass distribution.⁶⁸ It also provided a glimpse of North Korea's growing cyber capabilities and illustrated their willingness to use these capabilities. The next section highlights key examples of nation-states moving beyond these private sector targets, instead aiming at critical government functions in other countries.

C. CYBER-ATTACKS ON NATIONAL ASSETS

While many of the most notable cyber-attacks had private sector targets, some of the most devastating and costly cyber incidents involve state-sponsored attacks on

⁶⁴ "Law Enforcement Says Yahoo Account Hacks were Likely Sponsored by Foreign Government," CBS News, December 15, 2016, <http://www.cbsnews.com/news/yahoo-hack-law-enforcement-believes-state-actor-us-official-says/>.

⁶⁵ Ibid.

⁶⁶ Elizabeth Weise, "Yahoo Says 2013 Hack Hit All 3 Billion User Accounts, Triple Initial Estimates," USA Today, October 3, 2017, <https://www.usatoday.com/story/tech/2017/10/03/3-billion-yahoo-users-breached-company-says/729155001/>.

⁶⁷ Gabriel Sanchez, *Case Study: Critical Controls that Sony Should Have Implemented*, SANS Institute, June 1, 2015, <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022>.

⁶⁸ Ibid.

government systems.⁶⁹ In 2010, Iran discovered that a complex computer worm, known as Stuxnet, had infected the supervisory control and data acquisition (SCADA) system and programmable logic controllers in their nuclear research computer systems.⁷⁰ The worm utilized four zero-day security exploits, which are unknown vulnerabilities in software or hardware.⁷¹ These vulnerabilities have no patch because developers do not know they exist and it can sometimes take days, months, or years for developers or system administrators to discover and patch these weaknesses.⁷² Stuxnet was in Iran's nuclear systems for years, slowly altering the spin of the system's centrifuges, which caused them to spin out of control and destroy themselves.⁷³ The attack set Iran's nuclear program back several years and is widely described as "the world's first digital weapon."⁷⁴ While no one took credit for Stuxnet, experts believe the United States and Israel developed the worm and used an employee within the Iranian nuclear program to upload the worm to Iran's computer systems.⁷⁵

Any discussion of state-sponsored cyber operations must include two of the most active countries in cyberespionage and cyber warfare, Russia and China.⁷⁶ One example of Chinese-sponsored cyberespionage is the 2015 cyber-attacks of the United States' Office of Personnel Management (OPM). According to the United States, the Chinese

⁶⁹ Tavish Vaidya, *2001-2013: Survey and Analysis of Major Cyberattacks*, Georgetown University, September 1, 2015, <https://arxiv.org/pdf/1507.06673.pdf>.

⁷⁰ David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 26, 2013, <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

⁷¹ Ryan Naraine, "Stuxnet Attackers Used 4 Windows Zero-day Exploits," *ZD Net*, September 14, 2010, <http://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/>.

⁷² "What is a Zero-Day Exploit," *Fire Eye*, accessed November 4, 2017, <https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html>.

⁷³ David E. Sanger, "Obama Order Sped up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all.

⁷⁴ Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.

⁷⁵ Nate Anderson, "Confirmed: US and Israel Created Stuxnet, Lost Control of it," *Ars Technica*, June 1, 2012, <https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/>.

⁷⁶ Daniel Coats, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, May 11, 2017, <https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf>.

military penetrated OPM systems and stole the PII of over 20 million federal employees.⁷⁷ While some hackers penetrate systems for specific information or to disrupt certain elements within a system, China is well known for casting a wide web during cyber intrusions, hoping to acquire any and all available data.⁷⁸ Therefore, many experts believe China supported the attack to gather information on federal employees and develop a massive database they could later use to identify and recruit American spies within the federal government.⁷⁹

On the other hand, Russia is known for using their impressive cyber capabilities on specific targets.⁸⁰ As Michael Schmidt and David Sanger of the New York Times stated in early 2015, “While Chinese hacking groups are known for sweeping up vast amounts of commercial and design information, the best Russian hackers tend to hide their tracks better and focus on specific, often political targets.”⁸¹ Later that year, Russia demonstrated this targeted approach during a territorial dispute with Ukraine.⁸² Here, Russian hackers penetrated and disabled Ukraine’s power grid, knocking six Ukrainian power companies offline.⁸³ While certainly not the first example of cyber warfare, it was the first time a country aimed a cyber-attack directly at a civilian population.⁸⁴ The attack was a significant escalation in the ever-evolving world of cyber warfare and set the stage for future Russian cyber operations. A year later, Ukraine again blamed Russia for a

⁷⁷ Brian Naylor, “One Year After OPM Data Breach, What has Government Learned,” NPR, June 6, 2016, <http://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned>.

⁷⁸ Michael S. Schmidt and David E. Sanger, “Russian Hackers Read Obama’s Unclassified Emails, Officials Say,” New York Times, April 25, 2015, https://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html?_r=2.

⁷⁹ Brendan I. Koerner, “Inside the Cyberattack that Shocked the US Government,” Wired, October 23, 2016, <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>.

⁸⁰ Schmidt and Sanger, “Russian Hackers Read Obama’s Unclassified Emails, Officials Say.”

⁸¹ Ibid.

⁸² Evan Perez, “U.S. Official Blames Russia for Power Grid Attack in Ukraine,” CNN Politics, February 11, 2016, <http://www.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/>.

⁸³ Ibid.

⁸⁴ Ibid.

cyber-attack on Kiev's power grid.⁸⁵ Earlier this year Ukraine accused Russian hackers of a third series of attacks, this time disrupting their power grid, financial system and critical infrastructure systems.⁸⁶ The attacks demonstrate a willingness for world powers to expand their targets from federal government facilities and systems, like nuclear programs and employee personnel databases, to critical infrastructure that services the civilian population.

D. CYBER-ATTACKS ON STATE AND LOCAL GOVERNMENT ASSETS

While a cyber arms race is certainly an alarming trend for world leaders, another growing movement that should worry policymakers is organized cyber-attacks on state and local governments.⁸⁷ Malicious actors have a variety of motives for penetrating state and local information systems, but one of the most prevalent motives in recent incidents is data theft. For example, since 2014, the Oregon Employment Department and the state of Louisiana have both fell victim to data theft, which resulted in over one-million user profiles being compromised and released on the Dark Web.⁸⁸ These files included PII, such as social security numbers and addresses, which could be used to steal victims' identities or exploit key government officials.⁸⁹

Another common objective in recent cyber-attacks on state and local governments is hacktivism, which is a politically motivated attack on information system, designed to obstruct normal computer activity.⁹⁰ These attacks can come in various forms and from numerous malicious actors, but many of the most notable incidents were orchestrated by a decentralized hacktivism group known as Anonymous. For example, following the

⁸⁵ Pavel Polityuk, "Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid," Reuters, December 20, 2016, <http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF>.

⁸⁶ Natalia Zinets, "Ukraine Charges Russia with New Cyber Attacks on Infrastructure," Reuters, February 15, 2017, <http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN>.

⁸⁷ *Cyber Threats Facing State and Local Government*, Accenture Consulting, 2016, https://www.accenture.com/t20170203T030414__w_/us-en/_acnmedia/PDF-41/Accenture-NASCIO-Cyber-POV-v02.pdf.

⁸⁸ Ibid.

⁸⁹ Ibid.

⁹⁰ "What is Hacktivism," Stanford University, accessed November 4, 2017, <https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html>.

officer-involved shooting of teenager Michael Brown in Ferguson, Missouri, Anonymous orchestrated a multifaceted cyber-attack on the Saint Louis County Police Department and Ferguson city hall.⁹¹ The hacktivists stole police personnel records and coordinated distributed denial of service (DDOS) attacks on city systems, which affected system operations for several city offices.⁹²

Similarly, in 2015, Baltimore police arrested Freddie Gray for allegedly possessing an illegal switchblade.⁹³ Gray died from significant spinal injuries while in police custody, which sparked protests across the nation and motivated a group affiliated with Anonymous to initiate “Operation Baltimore,” a series of cyber-attacks that knocked the city’s website offline for over 16 hours.⁹⁴ Baltimore was unprepared for the cyber-attacks and struggled to keep online services running during the incident, but eventually returned to operation with assistance from the federal government.⁹⁵ In 2016, Anonymous continued to attack state and local information systems following the Flint, Michigan, water crisis and the passage of a controversial bill restricting the rights of transgender individuals in North Carolina.⁹⁶ These incidents highlighted the growing trend of hacktivism aimed at state and local governments, as well as a disturbing lack of

⁹¹ Dara Kerr, “Ferguson, Mo., Police Site Hit with DDoS Attack,” CNET, August 14, 2014, <https://www.cnet.com/news/st-louis-police-website-suffers-ddos-attack/>.

⁹² Ibid.

⁹³ “Freddie Gray’s Death in Police Custody – What we Know,” BBC, May 23, 2016, <http://www.bbc.com/news/world-us-canada-32400497>.

⁹⁴ “New Documents Show Cyber Hackers Struck Baltimore Days after Riots,” CBS Baltimore, July 31, 2015, <http://baltimore.cbslocal.com/2015/07/31/new-documents-show-cyber-hackers-struck-baltimore-after-riots/>.

⁹⁵ Ian Duncan, “City Faced Cyberattacks amid Chaos and Unrest on the Streets,” Baltimore Sun, July 31, 2015, <http://www.baltimoresun.com/news/maryland/sun-investigates/bs-md-ci-cyber-riot-20150731-story.html>.

⁹⁶ Gary Ridley, “Flint Hospital Confirms ‘Cyber Attack,’ Anonymous Threatens Action over Water Crisis,” Michigan Live Media Group, January 22, 2016, http://www.mlive.com/news/flint/index.ssf/2016/01/flint_hospital_confirms_cyber.html.

Colin Wood, “Unmasking Hacktivism and Other High-Profile Cyberattacks,” Gov Tech, August 28, 2015, <http://www.govtech.com/public-safety/Unmasking-Hacktivism.html>.

cyber preparedness by these government offices.⁹⁷ In each case, they were overwhelmed by the attacks and struggled to maintain online operations during the incidents.⁹⁸

Moreover, not all cyber incidents originate from a computer. In 2013, heavily armed and highly trained gunmen attacked Pacific Gas and Electric Company's Metcalf Transmission Substation in California, cutting fiber-optic phone lines and firing more than 100 rounds into the radiators of 17 transformers.⁹⁹ The attack briefly disabled the region's telecommunication systems, including their 9-1-1 emergency system, and resulted in \$15 million in damage.¹⁰⁰ One government official called the attack, "the most significant incident of domestic terrorism involving the grid that has ever occurred."¹⁰¹ It was a powerful example of a physical attack causing significant cyber consequences.¹⁰²

Overall, cyber incidents have evolved significantly since the *Morris* worm and the *Melissa* virus. While early cyber incidents could be inconvenient and unsettling, consequences were limited because systems were isolated and independent. As society progresses and technology evolves, the severity of these incidents continue to rise because information systems are increasingly interconnected and interdependent. Today's significant cyber incidents may have serious impacts on critical infrastructure systems, such as the power grid, or neutralize advanced nuclear programs, such as Stuxnet. Therefore, all levels of government must understand these threats and develop the cyber capabilities required to mitigate consequences and ensure continuity of operations. The next section examines the federal government's cyber preparedness policies and programs, which frame national cyber incident response efforts and support state and local cyber activities.

⁹⁷ Ibid.

⁹⁸ Ibid.

⁹⁹ Jose Pagliery, "Sniper Attack on California Power Grid May Have Been 'an Insider,' DHS Says," CNN Technology, October 17, 2015, <http://money.cnn.com/2015/10/16/technology/sniper-power-grid/>.

¹⁰⁰ Richard A. Serrano and Evan Halper, "Sophisticated but Low-tech Power Grid Attack Baffles Authorities," Los Angeles Times, February 11, 2014, <http://www.latimes.com/nation/la-na-grid-attack-20140211-story.html#page=1>.

¹⁰¹ Ibid.

¹⁰² Ibid.

E. FEDERAL PREPAREDNESS POLICIES

The foundation of national preparedness centers on the Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA), which created the National Preparedness System.¹⁰³ The National Preparedness System is a systematic process for developing the capabilities necessary to achieve the “National Preparedness Goal” of “a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.”¹⁰⁴ This system creates a structure for identifying threats, examining the capabilities required to manage these threats, and pinpointing methods to measure the maturity of these capabilities.

Federal readiness policies also build on *PPD 8: National Preparedness*, which outlines the actions required to build and sustain the preparedness capabilities described in the “National Preparedness Goal.”¹⁰⁵ PPD-8 requires DHS to maintain a series of plans organizing and aligning strategies “across the five mission areas: prevention, protection, mitigation, response, and recovery.”¹⁰⁶ These plans, known as the “National Planning Frameworks” and the “Federal Interagency Operational Plans,” are critical to the implementation of the National Preparedness System because they provide structure to a complex initiative that requires coordination from the whole community.¹⁰⁷ This structure allows everyone from a large federal agency to a small town to understand their role in enhancing national preparedness.¹⁰⁸

¹⁰³ “National Preparedness System,” FEMA, November 2011, https://www.fema.gov/media-library-data/20130726-1855-25045-8110/national_preparedness_system_final.pdf.

¹⁰⁴ “National Preparedness Goal,” FEMA, September 2015, https://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf.

¹⁰⁵ Barack Obama, “Presidential Policy Directive – National Preparedness,” DHS, March 30, 2011, <https://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf>.

¹⁰⁶ “National Preparedness System.”

¹⁰⁷ The National Preparedness Goal defines whole community as “individuals and communities, the private and nonprofit sectors, faith-based organizations, and all governments (local, regional/metropolitan, state, tribal, territorial, insular area, and Federal).” “National Preparedness Goal.”

¹⁰⁸ *Ibid.*

Another critical element of the National Preparedness System is the “National Incident Management System” (NIMS), which outlines a consistent approach to facilitating coordination between all levels of government during an incident.¹⁰⁹ It is modeled after the “National Interagency Incident Management System” (NIIMS), which was designed by firefighters to manage large-scale wildfires in California and Arizona, but its incident response principles extend to the digital world as well.¹¹⁰ Today, NIMS is an essential tool for managing incidents with multiple agencies and is used throughout the country for large-scale incidents.¹¹¹ The federal government requires departments and agencies to adhere to NIMS principles, including when coordinating cyber incident response activities.¹¹²

F. FEDERAL CYBERSECURITY AND CRITICAL INFRASTRUCTURE POLICIES

In 2013, the White House released *PPD-21: Critical Infrastructure Security and Resilience*, which aims to strengthen the federal government’s relationship with private sector partners by improving information sharing processes and mechanisms.¹¹³ PPD-21 focuses on the public-private partnership because the federal government believes homeland security is a shared responsibility, especially since a large majority of critical infrastructure is privately owned.¹¹⁴ This partnership is further described in the NIPP, a national plan to synchronize infrastructure protection efforts, and implemented by Sector-Specific Agencies (SSA), which are the federal departments and agencies tasked with

¹⁰⁹ “National Incident Management System,” FEMA, December 2008, https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

¹¹⁰ Nick Brunacini, “NIMS or NIIMS,” Fire Rescue Magazine, July 30, 2009, <http://www.firerescuemagazine.com/articles/print/volume-1/issue-3/command-leadership/nims-or-niims.html>.

¹¹¹ “NIMS: Frequently Asked Questions,” FEMA, accessed November 4, 2017, <https://www.fema.gov/pdf/emergency/nims/nimsfaqs.pdf>.

¹¹² “National Cyber Incident Response Plan,” US-CERT, December 2016, https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

¹¹³ Barack Obama, “Presidential Policy Directive – Critical Infrastructure Security and Resilience,” White House Archives, February 12, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

¹¹⁴ “Critical Infrastructure Sector Partnerships,” DHS, accessed November 4, 2017, <https://www.dhs.gov/critical-infrastructure-sector-partnerships>.

leading federal coordination within their critical infrastructure sector.¹¹⁵ The NIPP also explains how critical infrastructure owners and operators can incorporate cybersecurity strategies into their protection efforts to ensure secure and resilience systems, especially as interdependencies continue to increase within critical infrastructure systems.¹¹⁶

On the same day President Barack Obama released PPD-21, he also signed *EO 13636: Improving Critical Infrastructure Cybersecurity*, which requires federal agencies to work with public and private partners to identify cyber risk management best practices and improve cyber threat information sharing.¹¹⁷ The directive also ensures that the DHS Chief Privacy Officer and the DHS Officer for Civil Rights and Civil Liberties assess privacy and civil liberties risks created by the functions outlined in EO 13636.¹¹⁸ EO 13636 plays a pivotal role in cybersecurity policy because it highlights the interdependencies of cybersecurity and critical infrastructure, while also demonstrating the growing importance of prioritizing cybersecurity as a national security threat.¹¹⁹

EO 13636 also required the National Institute for Standards and Technology (NIST) to develop a cyber risk management guide, which led to the “Framework for Improving Critical Infrastructure Cybersecurity” (Cybersecurity Framework).¹²⁰ The Cybersecurity Framework provides “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.”¹²¹ The document is scalable to organizations of all sizes, providing standards,

¹¹⁵ “National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience,” DHS, accessed November 4, 2017, https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

¹¹⁶ *Ibid.* at 8.

¹¹⁷ Obama, “Executive Order – Improving Critical Infrastructure Cybersecurity.”

¹¹⁸ *Ibid.*

¹¹⁹ *Ibid.*

¹²⁰ “Framework for Improving Critical Infrastructure Cybersecurity,” NIST, February 12, 2014, <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

¹²¹ Obama, “Executive Order – Improving Critical Infrastructure Cybersecurity.”

guidelines, and best practices that can improve the organization's cybersecurity posture regardless of the industry.¹²²

In 2015, the White House took another step towards improving federal cybersecurity efforts by releasing *EO 13691: Promoting Private Sector Cybersecurity Information Sharing*, which aimed to improve cyber information sharing across all levels of government and the private sector.¹²³ EO 13691 created Information Sharing and Analysis Organizations (ISAO) to facilitate the flow of information within the private sector and between the public and private sector.¹²⁴ ISAOs are modeled after Information Sharing and Analysis Centers (ISAC), which are information hubs used by the critical infrastructure community to improve communications between owners and operators.¹²⁵ ISAOs are meant to supplement, not supplant, existing information sharing mechanism, such as ISACs, critical infrastructure coordinating councils, fusion centers and InfraGard, while focusing specifically on cyber intelligence.¹²⁶

One year later, the Obama administration released their final cybersecurity directive, *PPD-41: United States Cyber Incident Coordination*, which explains how each federal department and agency with a cyber nexus coordinates their cyber incident response efforts.¹²⁷ PPD-41 also clarifies roles and responsibilities for each federal cyber operations center and describes how the three lead organizations for cyber—DHS, the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI)—coordinate during a cyber incident.¹²⁸ The directive is an

¹²² "Framework for Improving Critical Infrastructure Cybersecurity," page 13.

¹²³ Barack Obama, "Executive Order – Promoting Private Sector Cybersecurity Information Sharing," White House Archives, February 13, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.

¹²⁴ Ibid.

¹²⁵ "Information Sharing," DHS, accessed November 4, 2017, <https://www.dhs.gov/topic/cybersecurity-information-sharing>.

¹²⁶ Obama, "Executive Order – Promoting Private Sector Cybersecurity Information Sharing."

"More Information," InfraGard, accessed November 4, 2017, <https://www.infragard.org/Application/General/MoreInfo>.

¹²⁷ Obama, "Presidential Policy Directive – United States Cyber Incident Coordination."

¹²⁸ Ibid.

important step in formalizing the roles of each cyber entity in the federal government, which minimizes confusion during an incident and clarifies the responsibilities of each entity in the cyber mission space.¹²⁹

PPD-41 also required an update to the “National Cyber Incident Response Plan” (NCIRP), which details how the public and private sectors can develop the capabilities required to prepare for and respond to a significant cyber incident.¹³⁰ The NCIRP is a scalable and flexible document so its principles can be applied across all levels of government and in the private sector.¹³¹ A transparent federal government cyber response plan provides state and local governments with the information necessary to build their own plans because all levels of government understand what to expect from federal cyber incident response efforts.¹³² Furthermore, the NCIRP is the connective tissue for physical and cyber preparedness as it formalizes the alignment between PPD-41 and the National Preparedness System.¹³³

Soon after President Donald Trump took office, he issued *EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which calls on federal departments and agencies to conduct risk assessments of their information systems and identify ways to improve their current digital infrastructure.¹³⁴ The order also requires federal departments and agencies to align their cybersecurity protocols to NIST’s “Cybersecurity Framework.”¹³⁵ Finally, EO 13800 directs the federal government to work with the private sector to improve the cybersecurity of critical infrastructures, such as bridges and power grids.¹³⁶

¹²⁹ Ibid.

¹³⁰ “National Cyber Incident Response Plan.”

¹³¹ Ibid.

¹³² Ibid.

¹³³ Ibid.

¹³⁴ Donald Trump, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” White House, May 11, 2017, <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.

¹³⁵ Ibid.

¹³⁶ Ibid.

G. POLICY IMPLEMENTATION

Together, PPD-8, PPD-21, and PPD-41, along with EO 13636, EO 13691, and EO 13800 provide a comprehensive framework for how the federal government protects against and responds to cyber incidents. These documents are the foundation for national cyber strategies because they describe how the federal government plans to develop, sustain, and utilize capabilities, while also offering guidance for state and local governments on how to develop their cyber preparedness policies and strategies.

Two key mechanisms for developing, implementing, and evaluating preparedness capabilities are the “National Preparedness Report” (NPR) and the Homeland Security Preparedness Grant (HSPG) program. The NPR is an annual report organized by the Federal Emergency Management Agency (FEMA) that evaluates the preparedness efforts of all levels of government, using more than 450 data sources from various public and private sector organization, including 66 non-federal organizations.¹³⁷ It measures current capabilities against predetermined targets to identify capability gaps and highlight areas for improvement.¹³⁸ The NPR has identified cybersecurity as the most significant capability gap every year since it was first published in 2012, despite jurisdictions acknowledging cybersecurity as their greatest security concern.¹³⁹

The HSPG program is also a critical element of the National Preparedness System and PPD-8 because it is a tool for addressing state and local government capability gaps identified in the NPR.¹⁴⁰ In 2016, FEMA allocated over \$1.6 billion to state and local governments through these programs and another \$729 million through other non-disaster relief grants.¹⁴¹ While these grants provide state and local governments with the funding necessary to address critical capability gaps, states have discretion on how to allocate the

¹³⁷ “National Preparedness Report,” FEMA, March 30, 2016, https://www.fema.gov/media-library-data/1476817353589-987d6a58e2eb124ac6b19ef1f7c9a77d/2016NPR_508c_052716_1600_alla.pdf.

¹³⁸ Ibid.

¹³⁹ Ibid.

¹⁴⁰ “Preparedness (Non-Disaster) Grants,” FEMA, accessed November 4, 2017, <https://www.fema.gov/preparedness-non-disaster-grants>.

¹⁴¹ “Grant Program Directorate Information Bulletin No. 411a,” FEMA, November 30, 2016, https://www.fema.gov/media-library-data/1482424650311-62d42ea5e0fd5f392d819372ba003496/FY16_Prep_Grant_Allocations_IB411a_GPD_Approved_v508.pdf.

funds within their jurisdiction and the continued lag in cybersecurity capability development suggests current allocation strategies are not working.

There are also several important programs and functions that are critical to implementing cybersecurity and critical infrastructure protection policies, especially for information sharing. A key structure the federal government utilizes to gather and disseminate information is a fusion center.¹⁴² DHS describes a fusion center as, “A collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.”¹⁴³ Fusion centers serve as an information hub between federal agencies and state and local government entities, which allows all participants to gather, analyze, and share information across all levels of government in real-time.¹⁴⁴

Critical infrastructure coordination mechanisms—such as coordinating councils, ISACs, and ISAOs—are also important information sharing structures because they serve as information nerve centers between all levels of government and the private sector.¹⁴⁵ The critical infrastructure community utilizes coordinating councils to enhance the public-private partnership within a sector and across sectors by promoting open and continuous dialogue.¹⁴⁶ This not only improves situational awareness during steady state, but also improves the community’s ability to respond during an event.¹⁴⁷ ISACs and ISAOs offer many of the same information sharing benefits as fusion centers and coordinating councils but they are unique because they offer around-the-clock operation

¹⁴² “Baseline Capabilities for State and Major Urban Area Fusion Centers,” Department of Justice – Justice Information Sharing, September 2008, <https://it.ojp.gov/documents/d/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf>.

¹⁴³ Ibid.

¹⁴⁴ “National Network of Fusion Centers Fact Sheet,” DHS, accessed November 4, 2017, <https://www.dhs.gov/national-network-fusion-centers-fact-sheet>.

¹⁴⁵ “Critical Infrastructure Sector Partnerships.”

¹⁴⁶ For a complete list of the sector and cross-sector council structures, see page 12 of NIPP 2013. See “National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience,” page 12.

¹⁴⁷ Ibid.

centers to private sector partners.¹⁴⁸ These operation centers provide situational awareness for critical infrastructure owners and operators and, when necessary, offer threat warning and incident reporting capabilities.¹⁴⁹ ISAOs differ from ISACs because they do not organize through the critical infrastructure sectors, which is useful to entities with cybersecurity interests that do not fit neatly within any of the 16 critical infrastructure sectors.¹⁵⁰

H. CONCLUSION

Overall, the federal government has developed a wide range of policies and programs to protect the nation against the evolving cyber threat landscape. While the various frameworks described in this chapter have not eliminated cyber risks, these efforts have improved the nation's ability to protect against and respond to significant cyber incidents. However, today's cyber threat environment is too interconnected and complex for the federal government to tackle alone. The job of protecting cyber assets must involve government at all levels. The next chapter outlines state and local government initiatives aimed at protecting key systems and infrastructure across the country, while also highlighting important gaps state and local governments must address to improve their cyber posture.

¹⁴⁸ "About ISACs," National Council of ISACs, accessed November 4, 2017, <https://www.nationalisacs.org/about-isacs>.

¹⁴⁹ Ibid.

¹⁵⁰ "Information Sharing and Analysis Organizations (ISAOs)," DHS, accessed November 4, 2017, <https://www.dhs.gov/isao>.

THIS PAGE INTENTIONALLY LEFT BLANK

III. OVERVIEW OF STATE AND LOCAL CYBER CAPABILITIES

As the scope and severity of cyber threats continues to grow, the role of state and local governments in addressing these threats becomes increasingly important. Cybersecurity was once a problem reserved for the federal government and the private sector, but today state and local governments are the first line of defense, especially if the cyber incident affects public services or critical infrastructure.¹⁵¹ State and local governments have tackled this challenge with varying degrees of success; therefore, this chapter examines how to build state and local government cyber capabilities to ensure they all have the tools to address this growing threat.

The first section of this chapter outlines the three most significant barriers state and local governments face when attempting to develop cyber capabilities: understanding the threat, allocating sufficient resources to address the threat, and developing a workforce capable of protecting against and responding to the threat. The second section describes current policies and programs state and local governments develop to overcome these barriers, including governments that have found success and governments that still struggle to overcome these obstacles. The third section identifies best practices and outlines a desired end-state for states as they continue developing their cyber strategies.

A. BARRIERS TO CYBER CAPABILITY BUILDING

While state and local governments understand the importance of cybersecurity, many still have difficulty developing the capabilities necessary to address this expanding threat. The NPR, which evaluates the capabilities of all 50 states based on self-assessments, has ranked cybersecurity as the most significant capability gap for five straight years despite states ranking cybersecurity as one of their highest priorities.¹⁵² In other words, states recognize the need to develop their cyber capabilities, but still struggle to improve their proficiency in cybersecurity.

¹⁵¹ Michael Daniel, “State and Local Government Cybersecurity,” White House Archives, April 2, 2014, <https://obamawhitehouse.archives.gov/blog/2014/04/02/state-and-local-government-cybersecurity>.

¹⁵² “National Preparedness Report.”

1. Understanding the Threats and Vulnerabilities

One factor that limits some state and local governments from strengthening their cybersecurity is their difficulties understanding the full range of threats and vulnerabilities.¹⁵³ The threat itself is undeniable. One Pennsylvania official claims that malicious actors attempted to breach the state's information systems over 90 billion times in 2016.¹⁵⁴ Even if only a small fraction of these attempts had the potential to cause harm, that is still an alarming number.

Today, technology is deeply woven into the fabric of nearly all public services as everything from public transportation to public health relies on digital systems to operate. This interconnectivity improves efficiency, but also creates new security weaknesses. For example, in 2016, malicious actors infected the San Francisco Municipal Railway ticketing system with ransomware, disrupting commuters and temporarily forcing officials to run transportation services for free as technical support addressed the security breach.¹⁵⁵ As the monetization of cyber-attacks increases and the popularity of ransomware grows, state and local governments should expect more of these attacks on their information systems.

State and local governments also store large amounts of data on their citizens and employees—such as voter registration information, birth certificates, and tax filings—which makes them susceptible to data theft if not properly protected. For example, in 2013, Washington's state court database was hacked, resulting in over 160,000 people's social security number and driver's license information being compromised.¹⁵⁶ The following year, malicious actors gained access to over one-million health records stored

¹⁵³ 2016 *Deloitte-NASCIO Cybersecurity Study*, NASCIO, accessed November 4, 2017, <https://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf>.

¹⁵⁴ Andrew Blake, "Pennsylvania Endured 90 Billion Attempted Cyber Intrusions in 2017: Report," *Washington Times*, July 18, 2017, <http://www.washingtontimes.com/news/2017/jul/18/pennsylvania-suffered-90-billion-attempted-cyberat/>.

¹⁵⁵ Harriet Taylor, "Metro Transport Systems Eyed after Hack Attack in San Francisco," *CNBC*, November 28, 2016, <http://www.cnn.com/2016/11/28/cybersecurity-experts-.html>.

¹⁵⁶ Kelly Clay, "Washington State Courts Hacked: 160,000 Social Security Numbers Potentially Accessed," *Forbes*, May 10, 2013, <https://www.forbes.com/sites/kellyclay/2013/05/10/washington-state-courts-hacked-160000-social-security-numbers-potentially-accessed/#7f71701636fa>.

on a Montana Department of Public Health and Human Services database.¹⁵⁷ State and local governments are being attacked on a daily basis, which makes every government information system vulnerable to a data breach and make state and local cyber capabilities even more important.¹⁵⁸

Additionally, a push to modernize state and local voting systems has left these governments vulnerable to voter fraud and election tampering, which threatens to undermine a key pillar in any democracy.¹⁵⁹ Assistant Secretary Jeanette Manfra of DHS's Office of Cybersecurity and Communications testified before Congress that 21 states had breaches to their election information systems during the 2016 presidential election.¹⁶⁰ Furthermore, 30 states used digital ballots that cannot be audited or verified by an independent monitor.¹⁶¹ While the United States intelligence community concluded that the cyber-attacks did not impact the election's results, malicious actors may be able to manipulate future elections if state and local governments are unable to strengthen their defenses and secure their systems.¹⁶²

As if the current threat environment were not challenging enough, cyber risks will only increase as emerging technologies become more commonplace in society, which will further strain security resources and increase the need for comprehensive cybersecurity policies. For example, many municipalities across the country are researching new technology that would move them closer to the smart city model.¹⁶³ The Department of Transportation defines smart cities as automated and integrated

¹⁵⁷ Laura Zuckerman, "Montana Health Record Hackers Compromise 1.3 Million People," Reuters, June 24, 2014, <http://www.reuters.com/article/us-usa-hacker-montana-idUSKBN0F006I20140625>.

¹⁵⁸ "Hacking a Problem for State Governments," Oregon Business Report, January 19, 2015, <http://oregonbusinessreport.com/2015/01/hacking-a-problem-for-state-governments/>.

¹⁵⁹ Jeanette Manfra, "Addressing Threats to Election Infrastructure," Senate Intelligence Committee, June 21, 2017, <https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF>.

¹⁶⁰ Ibid.

¹⁶¹ Jason Smith, "Digital Ballots, Outdated Machinery Leave Us Exposed to Russian Hack Round Two," USA Today, July 19, 2017, <https://www.usatoday.com/story/opinion/2017/07/19/digital-ballots-outdated-machinery-leave-us-exposed-second-russian-hack-jason-smith-column/487825001/>.

¹⁶² Manfra, "Addressing Threats to Election Infrastructure."

¹⁶³ "Smart City Challenge," Department of Transportation, accessed November 4, 2017, <https://www.transportation.gov/sites/dot.gov/files/docs/Smart%20City%20Challenge%20Lessons%20Learned.pdf>.

transportation systems that use data, applications, and technology to improve the movement of people within a city.¹⁶⁴ In 2014, New York City kicked off a smart city initiative to create a more responsive government by integrating information and communication technology through enhanced data collection of city assets and improved real-time information sharing.¹⁶⁵ This integration could greatly strengthen the efficiency and effectiveness of public services, but would also introduce new cyber risks, which allow failures in one system to have cascading impacts to other systems.¹⁶⁶

Similarly, the automotive industry is making significant progress in autonomous vehicle technology, which will revolutionize transportation for millions of Americans, but also create new cybersecurity risks. Ford and General Motors have each invested over one-billion dollars in artificial intelligence research, while technology companies like Google are also investing heavily in autonomous technology.¹⁶⁷ Furthermore, Uber is already test driving autonomous vehicles on public roads in Arizona, California, and Pennsylvania.¹⁶⁸ This technology is improving rapidly, but with these advancements comes new cybersecurity risks because it introduces new cyber vulnerabilities for malicious actors to exploit. Therefore, state and local governments must be prepared to develop strategies and policies that mitigate these risks ensure safety on their roads.

2. Inadequate Funding

Another obstacle limiting state and local governments from improving their cyber capabilities is difficulty securing sufficient resources to address capability gaps.¹⁶⁹ A 2016 study from the National Association of State Chief Information Officers (NASCIO)

¹⁶⁴ Ibid.

¹⁶⁵ “Building a Smart and Equitable City,” New York City Mayor’s Office of Tech and Innovation, accessed November 4, 2017, <http://www1.nyc.gov/site/forward/innovations/smartnyc.page>.

¹⁶⁶ Michael Totty, “The Rise of the Smart City,” Wall Street Journal, April 16, 2017, <https://www.wsj.com/articles/the-rise-of-the-smart-city-1492395120>.

¹⁶⁷ Alex Davies, “Detroit is Stomping Silicon Valley in the Self-driving Car Race,” Wired, April 3, 2017, <https://www.wired.com/2017/04/detroit-stomping-silicon-valley-self-driving-car-race/>.

¹⁶⁸ Robert Siegel, “Pittsburgh Offers Driving Lessons for Uber’s Autonomous Cars,” National Public Radio, April 3, 2017, <http://www.npr.org/sections/alltechconsidered/2017/04/03/522099560/pittsburgh-offers-driving-lessons-for-ubers-autonomous-cars>.

¹⁶⁹ 2016 Deloitte-NASCIO Cybersecurity Study.

surveyed each state's Chief Information Security Officer (CISO) about the levels of progress in their state's cybersecurity.¹⁷⁰ Only 10 CISOs said that cybersecurity is more than two percent of their information technology budget and only 12 states have at least 15 full-time employees working on cybersecurity.¹⁷¹ Furthermore, 80 percent of these CISOs believe they lack the funds necessary to provide appropriate security to the information systems in their jurisdiction.¹⁷²

One reason CISOs struggle to secure cybersecurity funding is that it is difficult to articulate the threat and why elected officials should prioritize cybersecurity costs alongside or above other public safety concerns, such as law enforcement or emergency services. State and local cybersecurity professionals struggle to maintain metrics that demonstrate effectiveness and convince decision-makers to reallocate resources. While some states, like New Mexico and Colorado, have robust cybersecurity plans that rely on data, other states do not provide clear measurements for success or risks.¹⁷³ This makes it more difficult to convince state leaders of the dangers associated with threats they may not understand or fully appreciate.

The result of this struggle is a “confidence gap” between elected officials and state cybersecurity leaders.¹⁷⁴ Roughly 66 percent of elected officials at the state level say they are very confident that their state has adequate cybersecurity policies and capabilities, while only 27 percent of state CISOs have this level of confidence.¹⁷⁵ These numbers suggest that subject matter experts have not been successful in teaching decision-makers about the scope and severity of the cyber threats their jurisdictions face.

Public officials are likely to continue prioritizing traditional services, like emergency services or road repair, because they understand these problems and

¹⁷⁰ Ibid. at 1.

¹⁷¹ Ibid. at 8.

¹⁷² Ibid. at 7.

¹⁷³ Gregory Dawson and Kevin C. Desouza, “How State Governments are Addressing Cybersecurity,” Brookings Institute, March 5, 2015, <https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/>.

¹⁷⁴ Ibid.

¹⁷⁵ Ibid.

appreciate their funding requirements. These traditional services also provide tangible results that allow taxpayers to see their tax dollars at work. For example, if a municipality repairs a pothole drivers see the road improvement, but most drivers do not think about the resources used to prevent malicious actors from breaching traffic light systems to cause harm. In general, voters do not assess politicians on their cybersecurity views unless the jurisdiction has been victimized by a security breach, thus politicians are not pressured to focus on these issues. Without proper metrics and education, state leaders will continue to deprioritize cybersecurity and focus resources elsewhere.

3. Workforce Gaps

A third barrier to improving cybersecurity at the state and local level is a lack of qualified candidates to fill information technology positions.¹⁷⁶ In 2015, the Bureau of Labor Statistics estimated there were more than 209,000 cybersecurity jobs in the United States.¹⁷⁷ Stanford University suggests that this number could grow 53 percent by the end of 2018.¹⁷⁸ Other experts believe the number of information security jobs could multiple tenfold by 2025.¹⁷⁹ This sharp upturn in demand will only increase the number of unfilled cybersecurity jobs, which will exceed 1.5 million across the world by 2020.¹⁸⁰ As the talent gap widens, competition for skilled cyber professionals will increase, which means state and local governments will only fall further behind if they do not develop strategies to overcome this barrier. Therefore, state and local governments should craft strategies to develop a pool of talented cybersecurity professionals able to fill the growing demand in the public and private sector.

¹⁷⁶ Ariha Setalvad, "Demand to Fill Cybersecurity Jobs Booming," Stanford University Peninsula Press, March 31, 2015, <http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/>.

¹⁷⁷ Ibid.

¹⁷⁸ Ibid.

¹⁷⁹ Ibid.

¹⁸⁰ "Cybersecurity Workforce Demand," National Initiative for Cybersecurity Education, accessed November 4, 2017, http://csrc.nist.gov/nice/NICE_Workforce_Demand.pdf.

B. CURRENT STATE AND LOCAL GOVERNMENT CYBER CAPABILITIES

As with many homeland security missions, state and local governments have varying levels of sophistication in cybersecurity. Some states have invested significant resources to build cyber capabilities and expand their state's footprint in the cybersecurity mission space, while other states are still working to build a foundation for future development. Since developing cyber capabilities is an inexact science, it is difficult to measure this divide. However, in 2013 the Potomac Institute for Policy Studies developed the *Cyber Readiness Index*, which is one of the first comprehensive studies examining the cyber capabilities of 125 countries across the world.¹⁸¹ This section uses their framework and tailors it to the state and local level to provide a common standard for analyzing the development of cyber capabilities in key areas.

The *Cyber Readiness Index* evaluates seven elements: (1) strategy; (2) incident response; (3) cybercrime and law enforcement; (4) information sharing; (5) research and development, education, and capacity building; (6) commerce; and (7) defense.¹⁸² These elements, while not exhaustive, are the pillars of a strong cyber foundation because they balance short and long-term needs. This positions jurisdictions for future growth, while still empowering them to address current cybersecurity concerns. The remainder of this section explores how state and local governments can enhance their capabilities in each of these categories.

1. Strategy

One critical component to short and long-term success in any homeland security mission is a well-developed strategy because it clarifies leadership objectives and outlines the path to achieve these objectives. A strategic plan allows state and local governments to prioritize operations and predict resource requirements, thereby

¹⁸¹ Melissa Hathaway, *Cyber Readiness Index 2.0*, Potomac Institute for Policy Studies, November 2015, page 4, <http://www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-index-2.0-web-2016.pdf>.

¹⁸² *Ibid.* at 4. Also, note that the *Cyber Readiness Index* identifies “diplomacy and trade” as an element, but diplomacy is largely a federal responsibility so this element was modified to “commerce,” which more closely aligns with the responsibilities of state and local governments.

stabilizing the budgetary process and minimizing inefficiencies.¹⁸³ Additionally, research from NASCIO suggests that states with formal cybersecurity strategies tend to receive more funding because they can articulate a clear plan to legislators.¹⁸⁴

As chairman of the National Governors Association (NGA), Virginia Governor Terry McAuliffe has worked to improve coordination between states as they develop and refine their cyber strategies.¹⁸⁵ The NGA, in collaboration with subject matter experts across the country, provide governors with “resources, tools and recommendations to help craft and implement effective state cybersecurity policies and practices.”¹⁸⁶ The association is also working with relevant stakeholders to create working groups that can offer guidance for state and local leaders to use when formulating their own cyber policy frameworks and plans.¹⁸⁷ Furthermore, the NGA issues recommended courses of action, such as *Act and Adjust: A Call to Action for Governors for Cybersecurity*, to facilitate the strategic planning process.¹⁸⁸

Some states have been successful incorporating these recommendations into their strategies. For example, Texas developed the *2016-2020 State Strategic Plan for Information Resources Management*, which outlines five strategic goals for ensuring the reliability and security of current public services, while also outlining paths for future innovation and workforce development.¹⁸⁹ Additionally, New Mexico developed a suite

¹⁸³ Jason Shueh, “For Funding, Colorado Cybersecurity Chief Says Strategy First,” State Scoop, March 13, 2017, <http://statescoop.com/for-funding-colorado-cybersecurity-chief-says-strategy-first>.

¹⁸⁴ *2016 Deloitte-NASCIO Cybersecurity Study*.

¹⁸⁵ “Gov. McAuliffe Named NGA Chair, Unveils Cyber Initiative,” National Governors Association, July 16, 2016, <https://www.nga.org/cms/news/2016/gov-mcauliffe-cyber-initiative>.

¹⁸⁶ “Resource Center for State Cybersecurity,” National Governors Association, accessed November 4, 2017, <https://www.nga.org/cms/center/issues/hsp/state-cybersecurity>.

¹⁸⁷ “Governors O’Malley and Snyder to Lead NGA Resource Center on Cybersecurity,” National Governors Association, October 2, 2012, https://www.nga.org/cms/home/news-room/news-releases/page_2012/col2-content/governors-omalley-and-snyder-to.html.

¹⁸⁸ “Act and Adjust: A Call to Action for Governors for Cybersecurity,” National Governors Association, September 2013, https://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf.

¹⁸⁹ “2016-2020 State Strategic Plan for Information Resources Management,” Texas Department of Information Resources, accessed November 4, 2017, <http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/2016-2020%20State%20Strategic%20Plan%20for%20Information%20Resources.pdf>.

of strategic plans, which are part of a long-term initiative to improve cyber capabilities in the public sector and private sector.¹⁹⁰ Overall, states with comprehensive cyber strategies are well-positioned to improve their cyber capabilities because they have a clear plan for the future. These strategies also provide a roadmap for resource allocation, which increases the likelihood of funding because decision makers understand what resources are necessary to facilitate growth and development.

2. Incident Response

Even the most secure information systems are vulnerable to a cyber-attack, which means that state and local governments must have adequate incident response capabilities to stop the attack and restore operations. This requires an incident response plan that identifies roles and responsibilities, as well as equipment and trained personnel to ensure that response efforts are organized and coordinated.¹⁹¹ Cyber incident response varies greatly from state to state, with some states using a multi-agency approach and others centralizing all responding entities into one unit.¹⁹² Other states have not formalized any cyber incident response strategy.¹⁹³ Each state must decide which approach best addresses their needs, while also understanding that a unity of effort allows states to maximize resources when addressing this growing threat.

One example of a state that uses a multi-agency approach to cyber incident response is Virginia.¹⁹⁴ During an incident, Virginia stands up a Unified Command Structure with three lead agencies—the Information Technologies Agency (ITA), the Department of Emergency Management, and the State Police—working together to manage the cyber and physical consequences of an incident.¹⁹⁵ The ITA is the lead

¹⁹⁰ “IT Strategic Planning,” New Mexico Department of Information Technology, accessed November 4, 2017, <http://www.doit.state.nm.us/strategicplanning.html>.

¹⁹¹ “Memo on State Cybersecurity Response Plans,” National Governors Association, accessed November 4, 2017, <https://ci.nga.org/files/live/sites/ci/files/1617/docs/MemoOnStateCybersecurityResponsePlans.pdf>.

¹⁹² Ibid.

¹⁹³ 2016 *Deloitte-NASCIO Cybersecurity Study*.

¹⁹⁴ “Memo on State Cybersecurity Response Plans.”

¹⁹⁵ Ibid.

authority on cyber response, while emergency managers and law enforcement handle the physical response.¹⁹⁶

On the other hand, Michigan takes a very different approach to cyber incident response through its Cyber Disruption Response Team (CDRT), which coordinates state response efforts to a cyber incident or disruption.¹⁹⁷ Like Virginia, the CDRT includes key leaders from emergency management, law enforcement and information technology, but instead of bringing multiple agencies together during an incident Michigan builds and trains interagency teams before an event so the teams can coordinate in advance.¹⁹⁸ This was successful during the Flint water crisis when hacktivists attempted to infiltrate the state's networks because the CDRT responded quickly and prevented any significant disruption of services.¹⁹⁹ As a result, this innovative approach to cyber incident response, while resource intensive, has become a model for other jurisdictions and the foundation for NASCIO's cyber incident planning guides.

States are also establishing teams of cyber reservists that are prepared to support primary incident response teams if an incident overwhelms existing resources. These support services can come from traditional reservist pools, like the National Guard, but some state and local governments are exploring civilian cyber emergency teams similar to the volunteer firefighter model.²⁰⁰ For example, Michigan created a Civilian Cyber Corps team, which is a group of trained cyber volunteers that provide emergency assistance when the governor declares a state of emergency.²⁰¹ While there is not enough evidence to determine whether these teams are capable of providing adequate support

¹⁹⁶ Ibid.

¹⁹⁷ "Cyber Disruption Response Team," State of Michigan, October 2015, http://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_Version_003_544764_7.pdf.

¹⁹⁸ Ibid. at 3.

¹⁹⁹ "2016 NASCIO Award Nomination: Michigan Cyber Disruption Response Plan," NASCIO, accessed November 4, 2017, https://www.nascio.org/portals/0/awards/nominations2016/2016/2016MI9-Cybersecurity_Cyber%20Disruption%20Response%20Plan%20NASCIO.pdf.

²⁰⁰ "Michigan Cyber Civilian Corps," State of Michigan, accessed November 4, 2017, http://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html.

²⁰¹ Ibid.

during an emergency, the program is an example of innovative solutions to the cybersecurity problem.

States have different approaches to managing cyber risks so the NGA surveyed each state's cyber incident response plan to categorize commonalities and identify best practices.²⁰² The NGA recognized that each state has different needs, but argued that all strong response plans have five essential elements: (1) clearly articulated authorities; (2) well-defined organizations, roles, and processes; (3) risk assessments; (4) coordination mechanisms across all relevant organizations; and (5) well-exercised response and recovery operations.²⁰³ These elements provide states with the information necessary to prepare for and respond to cyber incidents, while also accounting for the unique requirements and limitations of each jurisdiction.

3. Cybercrimes and Law Enforcement

The third element to consider when evaluating a state and local government's cyber capabilities is their legal authorities to prevent, investigate, and prosecute cybercrime. While industry experts and scholars define cybercrime differently, for the purposes of this thesis cybercrime is defined as "any crime that is committed using a computer or network, or hardware device."²⁰⁴ This may include data theft, fraud, copyright infringement, or any other illegal act that is executed through information systems.²⁰⁵ In 2015, cybercrimes cost victims roughly \$500 billion globally and that number is expected to rise to over two trillion dollars by 2019.²⁰⁶ Therefore, cybercrime is a serious concern to all levels of government throughout the world, one that will only grow as cybercriminals become more sophisticated and economies become more interconnected with the digital world.

²⁰² "Memo on State Cybersecurity Response Plans," 1-2.

²⁰³ Ibid.

²⁰⁴ "What is Cybercrime," Symantec Corporation, accessed November 4, 2017, <http://us.norton.com/cybercrime-definition>.

²⁰⁵ Ibid.

²⁰⁶ Bill Laberis, "20 Eye-Opening Cybercrime Statistics," Security Intelligence, November 14, 2016, <https://securityintelligence.com/20-eye-opening-cybercrime-statistics/>.

The Computer Fraud and Abuse Act (CFAA) limits the federal government's authority to prosecute cybercrimes unless there is a "compelling federal interest," which is "where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature."²⁰⁷ Therefore, in many cases it is incumbent upon state and local governments to have the expertise to investigate and prosecute cybercriminals. This responsibility is particularly challenging for police forces with resource limitations, inadequate cyber training, and inexperienced personnel.²⁰⁸ As a result, several states are taking steps to reallocate resources to address this growing problem.

Some states, such as Massachusetts, have drafted cybercrime strategies to organize state and local law enforcement agencies responding to and investigating these incidents.²⁰⁹ Other states have created new law enforcement agencies to handle these cases, which centralizes cybercrime responsibilities. For example, California—with a booming technology industry that is spearheaded by world renowned technology companies in Silicon Valley—created the California Cyber Crime Center to maximize law enforcement resources, enhance digital evidence capabilities, and promote innovation.²¹⁰ Other states have taken a similar approach with task forces, complaint centers, and other centralized programs designed to improve cybercrime investigations and maximize resources.

Overall, state and local governments must understand that cybercrime is a growing problem that requires a unique set of skills to prevent, investigate, and prosecute

²⁰⁷ "Prosecuting Computer Crimes," Office of Legal Education Executive Office for United States Attorneys, accessed November 4, 2017, <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>.

²⁰⁸ Martha Neil, "As State and Local Police Struggle to Investigate Cybercrime, Official Describes 'Helpless Feeling'," American Bar Association, April 21, 2014, http://www.abajournal.com/news/article/state_and_local_police_struggle_to_investigate_cybercrime/.

²⁰⁹ Maura Healey, "Cyber Crime Strategic Plan," Attorney General of Massachusetts, accessed November 4, 2017, <http://www.mass.gov/ago/public-safety/cyber-crime-and-internet-safety/cyber-crime-initiative/strategic-plan.html>.

²¹⁰ "California Cyber Crime Center," California Department of Justice, accessed November 4, 2017, <https://oag.ca.gov/c4>.

so traditional law enforcement models will not suffice.²¹¹ Many state and local governments are developing specialized teams or organizations to handle these complex cases, which is a step in the right direction but requires significant resources and training. Therefore, states must examine their laws and resources to ensure that these cybercrime operations have the tools necessary to manage these cases and punish cyber criminals.

4. Information Sharing

Information sharing is a critical component of all homeland security missions, but it is particularly important to cybersecurity because of the interconnectivity of systems and the agility of the cyber environment. Many information systems are also interdependent, which further amplifies the need for timely and actionable information sharing because most technology relies on the security of other systems for its own operability. Therefore, it is important that state and local government have mechanisms to share information with other government entities, as well as nongovernmental entities with cybersecurity interests.

There are several information sharing mechanisms for states to utilize—such as the federally sponsored ISACs, ISAOs, and fusion centers described in Chapter II and state-funded cyber centers—so each state must determine which tools, or groups of tools, meet their needs. For example, one information sharing service may focus on critical infrastructure vulnerabilities while another organization focuses solely on cyber threats in the financial sector. Therefore, states may need to gather information from multiple sources, which also means state and local governments must have the ability to understand how to manage these resources and use the information they receive to improve decision-making.

Some states have created their own cyber information sharing and operation centers to ensure the flow of timely and actionable information to public and private sector entities in their jurisdiction. For example, New Jersey created the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), to “promote shared and

²¹¹ Kristin Finklea and Catherine A. Theohary, “Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement,” Congressional Research Service, January 15, 2015, <https://fas.org/sgp/crs/misc/R42547.pdf>.

real-time awareness of cyber threats to New Jersey's citizens, local governments, businesses, and critical infrastructure owners and operators."²¹² The NJCCIC allows the state to promote cyber awareness, share information, file cyber incident reports, and analyze cyber threats.²¹³ While the information and analysis hub is still new, senior leaders in New Jersey's Office of Homeland Security and Preparedness believe the organization has given their agency the tools to address cyber threats in an organized and comprehensive fashion.²¹⁴ Other states, like Indiana, are following suit with their own operation centers to improve their cyber preparedness and cyber incident response efforts.²¹⁵

Overall, cyber's interconnected and global nature requires collaboration. There are many information sharing mechanisms for state and local governments, but governments need to understand how to maximize these resources and use this information to improve the cyber posture of all public and private sector entities in their jurisdiction. States that are successful sharing cyber information have developed strategies to take advantage of existing options and organize the information they receive into useful intelligence for their citizens.

5. Research and Development, Education, and Capacity Building

State and local governments must focus on the present but still have an eye on the future. The best way for governments to improve their cybersecurity future is to invest in cyber research and development, education and capacity building. These forward-thinking initiatives facilitate innovation and build the workforce required to meet the needs of a growing mission space. Some states, like California, have innovation ingrained in their culture, which allows them to lean on universities and the private sector to help

²¹² "Mission," NJ Cybersecurity and Communications Integration Cell, accessed November 4, 2017, <https://www.cyber.nj.gov/mission/>.

²¹³ Ibid.

²¹⁴ Eyrageon Eidam, "New Jersey Takes Consolidated, Fusion Center-Style Approach to Cybersecurity," Gov Tech, April 29, 2016, <http://www.govtech.com/security/New-Jersey-Takes-Consolidated-Fusion-Center-Style-Approach-to-Cybersecurity.html>.

²¹⁵ "Indiana Cybersecurity," Indiana, accessed November 4, 2017, <http://www.in.gov/cybersecurity/2402.htm>.

develop a cyber workforce.²¹⁶ However, other states do not have this luxury and need to take a more proactive approach to ensure that their jurisdiction offers an environment that cultivates innovation in technology.

Many state and local governments incentivize cyber education by offering scholarships to students pursuing cyber degrees or by providing grants to schools looking to research and develop new technology.²¹⁷ For example, Virginia recently developed a Cybersecurity Public Service Scholarship Program that awards one-million dollars in scholarships to Virginia students who study cybersecurity and work in the public sector after they graduate.²¹⁸ Virginia also offers technical training to military veterans searching for a post-military career in cybersecurity.²¹⁹ These programs eliminate the financial barriers to cyber education and improve the cyber skills of the current and future workforce.

Several states have also introduced cyber ranges, which are virtual reality environments where students can simulate cyber-attacks and practice defending their systems from malicious actors.²²⁰ Cyber ranges provide current and future cyber professionals with an opportunity to grow and develop their skills in a controlled but well-resourced facility.²²¹ These facilities also allow public and private sector organizations to train employees, try new software before purchasing, and test their network defenses in a safe environment that does not put real world systems at risk.²²²

²¹⁶ Andrea M. Hamilton, "Scholar Examines Links between Stanford, Silicon Valley," Stanford University, April 16, 2003, <http://news.stanford.edu/news/2003/april16/historysusv-416.html>.

²¹⁷ Francesca Spidalieri, *State of the States on Cybersecurity*, Pell Center for International Relations and Public Policy, 2015, <http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf>.

²¹⁸ "Governor McAuliffe Announces \$1 Million in Cybersecurity Scholarships," Virginia, accessed November 4, 2017, <https://governor.virginia.gov/newsroom/newsarticle?articleId=16192>.

²¹⁹ "Cyber Veterans Initiative," Cyber Virginia, accessed November 4, 2017, <http://cybervets.virginia.gov/>.

²²⁰ Gary Robbins, "USD Creating 'Cyber Range' to Train Students to Fight Digital Intruders," San Diego Union Tribune, October 6, 2016, <http://www.sandiegouniontribune.com/news/science/sd-me-cyber-range-20161005-story.html>.

²²¹ "Gov. McAuliffe Announces Creation of Virginia Cyber Range," Radford University, September 22, 2016, <http://www.radford.edu/content/radfordcore/home/news/releases/2016/september/gov--mcauliffe-announces-creation-of-virginia-cyber-range.html>.

²²² Ibid.

These programs alone will not bridge the cyber talent gap, but they are important steps that each jurisdiction can take to improve the technical skills of the next generation's workforce. States like Virginia and California have found success in training and developing their cyber workforce by offering an assortment of research and education options, which provides current and future cybersecurity professionals with opportunities to hone their skills. As a whole, all states should strive to develop their workforce by providing a range of options to research, learn, and train in the cybersecurity field.

6. Commerce

While technology saddles state and local governments with new security burdens, it also provides these jurisdictions with unlimited potential for economic growth. Cyber can alter existing industries, as demonstrated by technology's impact on the automotive industry with electric cars, or create new industries, such as the virtual reality or artificial intelligence industries.²²³ These advancements create new possibilities for local economies if local markets understand how to maximize new opportunities.

State and local governments have been racing to earn a stronghold in various technology industries, knowing that these industries are powerful job creators for cities across the world.²²⁴ For example, Maryland is one of many states to offer appealing pro-business incentives, including tax credits and seed money for startup technology companies, to lure companies to the region and increase the state's profile in the technology community.²²⁵ On the other hand, Detroit is luring top cyber professionals to their city with lower costs of living and remodeled business centers in the hopes that

²²³ "7 Fastest-Growing Industries to Invest in for 2016," NASDAQ, June 23, 2016, <http://www.nasdaq.com/article/7-fastestgrowing-industries-to-invest-in-for-2016-cm639446>.

²²⁴ Joel Kotkin and Mark Schill, "The Cities Creating the Most Tech Jobs 2017," *Forbes*, March 16, 2017, <https://www.forbes.com/sites/joelkotkin/2017/03/16/technology-jobs-2017-san-francisco-charlotte-detroit/#201597a38f6b>.

²²⁵ "IT and Cybersecurity in Maryland," Maryland Department of Commerce, accessed November 4, 2017, <https://open.commerce.maryland.gov/it-and-cybersecurity/>.

technology companies will follow the talent.²²⁶ Overall, the technology industry has demonstrated consistent growth throughout the 21st century, which means more jobs and a stronger economy for state and local governments that succeed in this market.²²⁷ Therefore, technology should not only be a high priority for security purposes, but also a key component of strategies for long-term job growth and a stable economy.

7. Defense

The final element of cyber preparedness is cyber defense because a state or local government's ability to protect itself from malicious actors is critical to their cybersecurity posture. The public relies on state and local governments to work with critical infrastructure owners and operators to protect critical systems in their jurisdiction, which means these entities must be able to provide support so these systems continue to operate. Furthermore, governments continue to put public services online, which leaves them vulnerable to cyber-attacks and increases the need to maintain a strong defensive cyber posture.

While no cyber defense is impenetrable, state and local governments must be able to minimize cyber risks, increase resilience, and ensure the integrity and reliability of essential information systems.²²⁸ As a result, cyber defense relies on the maturity of all other elements outlined in the *Cyber Readiness Index*. These governments must have comprehensive strategies that lead a coordinated effort to protect information systems and prevent cyber-attacks. Additionally, they must have a skilled workforce that is well-trained, well-informed, and equipped with the latest security products and tools, while also being able to respond quickly when a malicious actor does penetrate lines of defense. Overall, a strong cyber defense is the result of a commitment to developing all elements

²²⁶ Gina Hall, "How Detroit Automakers are Trying to Lure Away Silicon Valley Tech Talent," *Silicon Valley Business Journal*, May 9, 2017, <https://www.bizjournals.com/sanjose/news/2017/05/09/ford-gm-detroit-tech-hiring-silicon-valley-waymo.html>.

²²⁷ Barnard Marr, "Why Everyone Must Get Ready for the 4th Industrial Revolution," *Forbes*, April 5, 2016, <https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/#a719f1e3f90b>.

²²⁸ Spidalieri, "State of the States on Cybersecurity."

of cyber preparedness so governments need to enhance all of their cyber capabilities if they want strong cybersecurity.

C. STATE AND LOCAL GOVERNMENT BEST PRACTICES

The time has come for state and local governments to focus on building their own cybersecurity and cyber response capabilities. State and local governments have been victimized by everything from ransomware attacks on critical infrastructure to widespread cyber-attacks on voting systems, which illustrates the need to improve their cyber aptitude.²²⁹ Fortunately, several states have found success building cyber capabilities, which provides best practices for other state and local governments. States like Virginia, Maryland, Michigan, and California have set the bar for cyber preparedness at the state level and while each state has taken a unique approach, there are three trends other states should incorporate into their cyber capability building plans. These best practices include: (1) crafting comprehensive cyber strategies; (2) developing organizations that allow the state to implement these strategies; (3) and providing these organizations with the tools necessary to achieve their mission.

The states with the most advanced cyber capabilities have crafted comprehensive cyber strategies aimed at strengthening each of the seven elements outlined in the *Cyber Readiness Index*. A comprehensive cyber strategy is a critical first step for building cyber capabilities because it provides a blueprint for success by identifying short and long-term goals, as well as a path for achieving these goals. This allows states to develop policies and plans that help implement their strategies. Each state should develop a strategy that addresses their cyber risks, but also identifies opportunities for social and economic growth.

States have also found success in developing their cyber capabilities by developing organizations or programs that centralize functions and focus on maximizing resources and personnel. For example, California has redefined how law enforcement prosecutes cybercrimes by creating an organization dedicated to these specialized, and

²²⁹ “State of Cybersecurity in Local, State and Federal Government,” Federal Computer Week, accessed November 4, 2017, <https://fcw.com/pages/hpsp/hpsp-10.aspx>.

often complex, crimes. The California Cyber Crime Center centralizes cybercrime reporting and improves collaboration by allowing all law enforcement officers with cybercrime portfolios to share resources.²³⁰ This also allows California to offer advanced training in one location and provide state-of-the-art technology, such as digital forensics, that helps law enforcement as they investigate these crimes.²³¹ Many states run cyber operation centers that track cyber threat indicators and share information with partners in the public and private sector, which improves the state's ability to protect against and respond to cyber threats.

A comprehensive cyber strategy and an efficient cyber workforce are critical elements to building cyber capabilities, but these concepts only work if states provide the workforce with the tools they need to accomplish their mission. These tools should include state-of-the-art facilities and equipment that allow cyber professionals to keep pace with evolving technology, as well as training so the workforce has the skills necessary to combat a seemingly endless number of cyber threats. In the end, a workforce is only as strong as the tools it has to work with so states should ensure that their cyber professions are equipped to handle these complex threats.

As a whole, the most prepared states have comprehensive cyber strategies and the resources necessary to implement these strategies. These resources allow states to address cybersecurity issues without relying on the federal government or the private sector to assist, which empowers them to control their own destiny in an evolving digital world. If states follow these best practices and focus on building the seven capabilities identified in the *Cyber Readiness Index*, they will be well-positioned to handle future challenges and prosper from a growing industry.

D. CONCLUSION

As the first line of defense in many cyber incidents, particularly cyber incidents affecting public services and critical infrastructure, state and local governments must

²³⁰ "California Cyber Crime Center."

²³¹ *Ibid.*

have the capabilities necessary to protect against and respond to cyber-attacks. Currently, understanding the threat, inadequate funding, and workforce gaps are the obstacles that limit states from improving these capabilities, but these impediments can be overcome. In fact, some states are making significant progress in the cyber mission space and are well-positioned to meet the cybersecurity challenges of evolving technology, such as driverless vehicles and smart cities. Other states should follow their lead and prioritize cybersecurity as a top security issue.

Moving forward, the desired end-state for each state and local government should be to develop enough cyber capabilities to handle most cyber incidents without any interruption to government services, much like law enforcement and emergency services are able to handle most incidents without requiring assistance from the FBI or FEMA. States should also be able to protect their critical infrastructure from cyber-attacks and have the technical skills to assist private sector owners and operators when their systems are attacked. Chapter IV outlines the legal framework for this approach to cybersecurity and examines how other homeland security missions employ federalism principles to empower state and local governments.

IV. BUILDING A FRAMEWORK FOR JURISDICTIONAL BOUNDARIES IN CYBER

Since the American Revolution, U.S. leaders have been at odds over the proper balance of state sovereignty and a strong central government. While Article I of the Articles of Confederation created a centralized government, Article II ensured “each state retains its sovereignty, freedom, and independence, and every power, jurisdiction, and right, which is not... expressly delegated to the United States, in Congress assembled.”²³² These conflicting messages left uncertainty over the roles of the states and the federal government, which remained a lingering ambiguity when the Constitution replaced the Articles of Confederation.

While several provisions within the Constitution expanded the federal government’s power, other sections of the Constitution continued to protect states’ rights. For example, the Necessary and Proper Clause in Article I, which authorizes Congress to “make all Laws which shall be necessary and proper,” provides the legislative branch significant power to enact laws it believes serve the best interests of the country.²³³ Additionally, the Supremacy Clause in Article VI declares federal laws “the supreme Law of the Land,” which prevents states from enforcing any laws that conflict with federal statutes.²³⁴

On the other hand, the Constitution also ensures that states retain authority to govern their citizens. The strongest protection of state sovereignty stems from the 10th Amendment: “The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people.”²³⁵ This amendment empowers states by providing them the authority to enact the laws and policies that best meet the needs of their constituents.

²³² “Articles of Confederation,” Library of Congress, accessed November 4, 2017, <https://memory.loc.gov/cgi-bin/ampage?collId=llsl&fileName=001/llsl001.db&recNum=127>.

²³³ U.S. Const. art. I, § 8.

²³⁴ U.S. Const. art. VI, § 2.

²³⁵ U.S. Const. amend. X.

Together, these principles guide the jurisdictional balancing act among the various levels of government in the United States and provide a legal framework for each government's underlying authorities. The remainder of this chapter examines this ageless conflict and its impacts on cybersecurity by outlining current jurisdictional considerations for cyber and surveying other homeland security mission spaces for best practices.

A. LEGAL FRAMEWORKS

Federalism is the principle that authority to govern should be dispersed across multiple levels of government and not be vested in a single governing body.²³⁶ Justice Anthony Kennedy once argued that federalism is the framers' brilliant strategy for preventing authoritarian rule while allowing the country to reap the social and economic benefits of unified governance.²³⁷ He stated,

Federalism was our Nation's own discovery. The Framers split the atom of sovereignty. It was the genius of their idea that our citizens would have two political capacities, one state and one federal, each protected from incursion by the other. The resulting Constitution created a legal system unprecedented in form and design, establishing two orders of government, each with its own direct relationship, its own privity, its own set of mutual rights and obligations to the people who sustain it and are governed by it.²³⁸

Essentially, federalism was a unique experiment designed to protect against tyranny by providing authority to multiple layers of government, which also created endless ambiguity.

Several landmark cases have shaped the balance of power between federal and state governments. For example, in *Ware v. Hylton*, the Supreme Court held a Virginia statute that allowed the state to confiscate debt payments to English creditors was unconstitutional because it undermined a treaty between the United States and England, thereby violating the Supremacy Clause.²³⁹ While the Constitution grants states the right

²³⁶ *United States Term Limits, Inc. v. Thornton*, 514 U.S. 779, 1995 (Kennedy, J., concurring).

²³⁷ *Ibid.*

²³⁸ *Ibid.*

²³⁹ *Ware v. Hylton*, 3 U.S. 199, 1796.

to enact and enforce their own laws, the Court determined the federal government would triumph when state actions conflicted with federal laws and treaties. The holding of this case later became known as the preemption doctrine.²⁴⁰

The Supremacy Clause is critical to current cyber policies because it gives the federal government significant authority to enact cyber legislation and influence cyber policies across the country. It also impacts the ability of state and local governments to develop their own cybersecurity laws because these statutes must adhere to federal rules. For example, each state has its own laws concerning electronic communications but changes to federal laws on electronic communication, such as the Communications Assistance for Law Enforcement Act (CALEA), may invalidate these state statutes.²⁴¹ Therefore, the Supremacy Clause puts states in a precarious position because they risk allocating significant resources to developing and implementing comprehensive cyber policies, only to later have these policies undermined by contradictory federal policies.

The federal government also retains authority to control the flow of money between states through the Commerce Clause, which affirms that Congress has the power “to regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes.”²⁴² For example, in one of the most influential Commerce Clause cases in United States history, *Gibbons v. Ogden*, a New York statute allowed the state to lease exclusive rights to trade in its waters, which conflicted with federal interstate trade regulations.²⁴³ The Supreme Court again ruled in favor of the federal government, determining that the Commerce Clause prevented states from enacting laws that conflicted with federal interstate commerce legislation.²⁴⁴ This decision solidified the federal government’s broad authority to control the flow of commerce across the country.

²⁴⁰ Ibid.

²⁴¹ Edward C. Liu, Gina Stevens and Kathleen Ann Ruane, “Cybersecurity: Selected Legal Issues,” Congressional Research Service, April 17, 2013, <https://fas.org/sgp/crs/misc/R42409.pdf>.

²⁴² U.S. Const. art. I, § 8, clause 3.

²⁴³ *Gibbons v. Ogden*, 22 U.S. 1, 1824.

²⁴⁴ Ibid.

The emergence of e-commerce will play a significant role in how markets are regulated in the future. In 2016, e-commerce accounted for over 40 percent of all retail sales growth.²⁴⁵ During that year, over 224 million customers purchased items online, and the National Retail Federation expects online retail to grow between eight to 12 percent in 2017, which means total online sales will exceed \$400 billion.²⁴⁶ However, e-commerce is also blurring state lines and international borders because people can buy products from anywhere in world with the click of a button. As online banking and e-commerce become more prevalent, the security of these systems becomes more important so understanding which government has the authority to oversee these markets is critical. While states traditionally have authority to regulate commerce within their borders, the rise of e-commerce may strengthen the federal government's authority to regulate commerce because the interconnectivity of e-commerce increases the likelihood of a cyber incident in one state affecting citizens of another state. This dynamic may impact the traditional balance of power between the federal government and the states; therefore, it is important for all levels of government to find the proper balance to ensure that there are strong cybersecurity policies in place to support this growing industry.

While the Supremacy Clause and the Commerce Clause provide the federal government certain enumerated powers in jurisdictional disputes, the federal government also has implied powers created by the Necessary and Proper Clause. In *Federalist Paper 44: Restrictions on the Authority of the Several States*, James Madison notes that the Necessary and Proper Clause was the most controversial provision in the Constitution but a critical element because the clause gives the Constitution the flexibility required for longevity.²⁴⁷ He reasoned that no document could ever account for all current conditions

²⁴⁵ "U.S. Census Bureau News," Department of Commerce, May 16, 2017, https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

²⁴⁶ "National Retail Federation Estimates 8-12% US E-commerce Growth in 2017," Business Insider, February 10, 2017, <http://www.businessinsider.com/national-retail-federation-estimates-8-12-us-e-commerce-growth-in-2017-2017-2>.

²⁴⁷ James Madison, "Federalist Number 44," Congressional Resources, 1787, <https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-44>.

or predict all future issues; therefore, the Necessary and Proper Clause affords the federal government the ability to address problems as they arise.²⁴⁸

The Supreme Court's decision in *McCulloch v. Maryland* demonstrates the vast powers bestowed on the federal government by the Necessary and Proper Clause.²⁴⁹ Here, the state of Maryland aimed to impede the operations of a federal bank within its jurisdiction by taxing all notes associated with the bank, but the federal government refused to pay.²⁵⁰ The Court sided with the federal government, arguing that the Constitution grants the federal government certain implied powers through the Necessary and Proper Clause, including the power to create a national bank, and states cannot enact laws that impede these implied powers.²⁵¹

Aside from the creation of federal banks, one of the most significant examples of the federal government asserting authority through the Necessary and Proper Clause is President Franklin D. Roosevelt's New Deal initiative.²⁵² The New Deal was a series of programs aimed at guiding the United States through the Great Depression by increasing federal assistance programs and expanding the role of the federal government in governmental functions.²⁵³ Roosevelt used the Necessary and Proper Clause as the legal basis for his ambitious programs, reasoning that he needed to implement these programs to save a crumbling economy and ensure the nation's welfare.²⁵⁴ The New Deal brought fundamental and dramatic changes to the U.S. intergovernmental system because it introduced the widespread use of federal grant programs to influence state actions.²⁵⁵

²⁴⁸ Ibid.

²⁴⁹ *McCulloch v. Maryland*, 17 U.S. 316, 1819.

²⁵⁰ Ibid.

²⁵¹ Ibid.

²⁵² John Wallis and Wallace E. Oates, "The Impact of the New Deal on American Federalism," National Bureau of Economic Research, January 1998, http://www.colorado.edu/ibs/es/alston/econ8534/SectionX/Wallis_and_Oates,_The_Impact_of_the_New_Deal_on_American_Federalism.pdf.

²⁵³ Ibid.

²⁵⁴ Randy Barnett, "The Choice between Madison and FDR," *Georgetown University Law Center*, 2008, <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1840&context=facpub>.

²⁵⁵ Wallis and Oates, "The Impact of the New Deal on American Federalism."

Roosevelt required states to initiate certain programs or enact certain legislation to receive federal grants, which expanded the federal government's authority but also gave states additional resources to develop programs and provide services within their borders.²⁵⁶

As the New Deal demonstrated, the Necessary and Proper Clause gives the federal government wide discretion to implement federal programs if it is in the best interest of national security and public welfare. Therefore, as the nation becomes increasingly reliant on technology, cybersecurity becomes more important to public welfare, and the federal government's authority to organize cybersecurity programs strengthens. This principle also provides the federal government the authority to influence how state and local governments organize and operate their cyber operations—if these state and local governments accept cybersecurity grant funding. Therefore, the Necessary and Proper Clause may be the federal government's most powerful Constitutional tool for implementing cybersecurity policies while proving legal justification for granting funds to states in need of federal support.

On the other end of the spectrum, the 10th Amendment provides states significant authority to develop their own policies and enact their own laws. In fact, in *Federalist Paper 45: The Alleged Danger From the Powers of the Union to the State Governments Considered*, Madison proclaims, “The powers reserved to the several states will extend to all objects, which, in the ordinary course of affairs, concern the lives, liberties and prosperities of the people, and the internal order, improvement, and prosperity of the state.”²⁵⁷ Therefore, while the enumerated and implied powers give the federal government tremendous power, the states have their own powers to influence policy.

One landmark decision that demonstrates how the 10th Amendment protects states sovereignty is *New York v. United States*.²⁵⁸ In this case, a federal statute, known as the Low-Level Radioactive Waste Policy Amendments Act, required states to develop

²⁵⁶ Ibid. at 156.

²⁵⁷ James Madison, “Federalist Number 45,” Congressional Resources, 1787, <https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-45>.

²⁵⁸ *New York v. United States*, 505 U.S. 144, 1992.

comprehensive waste disposal plans and forced states to take ownership of the waste if private companies did not comply with these plans.²⁵⁹ New York enacted its own waste disposal legislation, which did not include the “take title” provision, and sued to stop the federal government from undermining state policies.²⁶⁰ The Supreme Court held that the federal government could not “commandeer” the state legislative process, thereby protecting New York’s right to create and enforce its own laws.²⁶¹

Later cases continued to magnify the 10th Amendment’s power in protecting state sovereignty and limiting federal overreach. For example, in *Printz v. United States*, the Brady Act required state and local law enforcement officers to run background checks on prospective handgun purchasers.²⁶² The Supreme Court held that requiring states to enforce federal law impeded on state sovereignty.²⁶³ The Court reached a similar verdict in *Shelby County v. Holder*, when several states challenged a provision in the Voting Rights Act that required select southern states to obtain federal approval before making changes to their voting laws.²⁶⁴ Chief Justice John Roberts concluded that the provision violated the principle of “equal sovereignty” and the states’ ability to pursue their own legislative objectives.²⁶⁵

Overall, the Constitution grants the federal government broad authority to create and enforce federal laws, but the 10th Amendment also provides the states significant power to govern within their borders. While there are limitations to a state’s authority to develop, implement, and enforce cyber laws and policies, the 10th Amendment gives states wide discretion to manage the mission space as they see fit. As a result, the federal government and the states have a complimentary, though sometimes hostile, relationship

²⁵⁹ Ibid.

²⁶⁰ Ibid.

²⁶¹ Ibid.

²⁶² *Printz v. United States*, 521 U.S. 898, 1997.

²⁶³ Ibid.

²⁶⁴ *Shelby County v. Holder*, 570 U.S. ___, 2013.

²⁶⁵ Ibid.

whereby each governing body aims to stay within its constitutional limits while still providing services to its constituents.

B. FEDERALISM IN OTHER HOMELAND SECURITY MISSIONS

The jurisdictional balancing act is common to homeland security because all levels of government play an important role. Long before Congress created the Department of Homeland Security (DHS) in 2003, many of the nation’s most important homeland security functions were performed by police officers, firefighters, and other first-responders. After DHS was created, the lines of power blurred, but state and local authorities remained a critical cog in the security machine. This section focuses on the role of federalism in three missions—counterterrorism, immigration enforcement, and emergency management—to determine what lessons cyber professionals can learn about balancing the homeland security interests of all levels of government.

1. Counterterrorism

Terrorism is a complex threat that requires coordination and information sharing across all levels of government but also creates friction and confusion when law enforcement agencies respond to the same incident or conduct overlapping investigations. While the mission space relies heavily on the basic principles of the Supremacy Clause and the 10th Amendment, there are statutes and policies that define the appropriate lanes for each level of government. Article III, Section 1, of the Constitution states, “The judicial power of the United States, shall be vested in one Supreme Court, and in such inferior courts as the Congress may from time to time ordain and establish.”²⁶⁶ In 1789, Congress used this authority to establish a federal court system by enacting “An Act to Establish the Judicial Courts of the United States,” also known as the Judiciary Act.²⁶⁷ The Judiciary Act gave federal courts exclusive jurisdiction over federal law violations.²⁶⁸ However, as the nation grew federal prosecutorial resources thinned so

²⁶⁶ U.S. Const. art. III, § 1.

²⁶⁷ “Judiciary Act of 1789,” Library of Congress, accessed November 4, 2017, <https://www.loc.gov/rr/program/bib/ourdocs/judiciary.html>.

²⁶⁸ Ibid.

Congress gave states concurrent jurisdiction, thereby allowing them to try criminal cases that violated both state and federal law.²⁶⁹

Today, Title 18 of the United States Criminal Code specifies that “the district courts of the United States shall have original jurisdiction, exclusive of the courts of the States, of all offenses against the laws of the United States”; however, it also notes that this authority does not impair state courts’ jurisdiction of criminal cases.²⁷⁰ This statute formalizes the concurrent jurisdiction structure whereby, in certain circumstances, federal courts and state courts can each prosecute criminals for the same crime. As a result, concurrent jurisdiction empowers states to create and enforce their own laws, thereby strengthening state sovereignty, but it also increases the need for coordination between levels of government to ensure the efficient use of resources.

The United States Criminal Code also creates certain rules for determining which level of government has the authority to prosecute the most serious crimes, such as terrorism. The federal government has exclusive jurisdiction to prosecute a terrorist act if the act “transcends national boundaries.”²⁷¹ However, states have exclusive jurisdiction if the act is considered domestic terrorism under state law and has no foreign nexus.²⁷² Other terrorism crimes, such as the use of weapons of mass destruction, provide federal and state governments with concurrent jurisdiction.²⁷³ If both levels of government have jurisdiction, the FBI works with relevant state and local law enforcement agencies to investigate and prosecute the crime. This collaboration takes place in many forms but the FBI’s Joint Terrorism Task Forces (JTTF) and fusion centers often play an important role.²⁷⁴

²⁶⁹ Ibid.

²⁷⁰ *Violent Crime Control and Law Enforcement Act*, 18 U.S. Code 211 § 3231.

²⁷¹ *Antiterrorism Act*, 18 U.S. Code 113B § 2332b.

²⁷² Lisa Daniels, “Prosecuting Terrorism in State Court,” Lawfare Blog, October 26, 2016, <https://www.lawfareblog.com/prosecuting-terrorism-state-court>.

²⁷³ *Antiterrorism Act*, 18 U.S. Code 113B § 2332a.

²⁷⁴ Kristin M. Finklea, “The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement.”

The complexities of overlapping authorities illustrates the importance of clear jurisdictional boundaries across all levels of government. Cyber policymakers can learn from law enforcement by pushing for laws and policies that outline roles and responsibilities in the cyber mission space. While PPD-41 outlines responsibilities for each federal agency in the cyber mission space, there are no statutes outlining jurisdictional boundaries between federal and state agencies. This gap leaves ambiguity and the potential for conflict, which strains relationships and hinders communication and collaboration.

2. Immigration Enforcement

Immigration enforcement was once seen as a federal government responsibility, with state and local governments having little influence on immigration laws and policies, but a rise in migration has forced this dynamic to change.²⁷⁵ In 2015, there were over 11 million undocumented immigrants in the United States, which suggests the federal government alone did not have the manpower required to enforce immigration laws.²⁷⁶ As a result, the federal government asked the states for assistance—something many scholars now refer to as immigration federalism—but not all states and cities have complied because of fundamental disagreements over the policies being enforced.²⁷⁷

This controversy over state enforcement of federal immigration laws has led to sanctuary cities, jurisdictions that do not detain unauthorized immigrants simply because of their immigration status.²⁷⁸ Sanctuary cities maintain that the federal government does

²⁷⁵ Jennifer Chacon, “Who is Responsible for U.S. Immigration Policy?” American Bar Association, accessed November 4, 2017, https://www.americanbar.org/publications/insights_on_law_and_society/14/spring-2014/who-is-responsible-for-u-s-immigration-policy-.html.

²⁷⁶ Jens Manuel Krogstad, Jeffrey S. Passel, and D’Vera Cohn, “5 Facts about Illegal Immigration in the U.S.,” Pew Research Center, April 27, 2017, <http://www.pewresearch.org/fact-tank/2017/04/27/5-facts-about-illegal-immigration-in-the-u-s/>.

²⁷⁷ Barbara E. Armacost, “‘Sanctuary’ Laws: The New Immigration Federalism,” Michigan State Law Review, 2016, https://static1.squarespace.com/static/55549704e4b0565df9f2305b/t/5899e9ea9de4bb90ccdae372/1486481898620/01_Armacost_Soft+Edits.pdf.

²⁷⁸ Janell Ross, “6 Big Things to Know about Sanctuary Cities,” Washington Post, July 8, 2015, https://www.washingtonpost.com/news/the-fix/wp/2015/07/08/4-big-things-to-know-about-sanctuary-cities-and-illegal-immigration/?utm_term=.24508cc0b875.

not have the authority to mandate that state officials enforce federal laws on behalf of the government, as the Supreme Court held in *Printz v. United States*.²⁷⁹ Therefore, while the Supremacy Clause prevents states from enacting laws that conflict with federal immigration laws, the 10th Amendment protects the states from being forced to act as agents for the federal government.

However, as demonstrated by President Roosevelt in the New Deal, the Necessary and Proper Clause gives the federal government the authority to attach conditions to federal grants. As a result, President Donald Trump has threatened to eliminate federal grants to sanctuary cities until they agree to enforce immigration laws.²⁸⁰ In sum, the current immigration enforcement dispute highlights the importance of clarifying jurisdictional boundaries for homeland security matters and illustrates the problems that arise when all levels of government fail to formalize these limits.

From a cyber perspective, this delicate balance between the federal powers and states' rights in immigration enforcement demonstrates the complexities of protecting state sovereignty, while maintaining homeland security. Whereas the federal government has significant authority to create cyber policies, states have the ability to limit the effectiveness of these policies. Therefore, it behooves all levels of government to work together on policies and strategies that protect the interests of each partner, to ensure efficient and effective implementation.

3. Emergency Management

For decades, federalism has been a driving force in determining emergency management policies and procedures. Following a string of poorly handled disaster response efforts in the 1970s, President Jimmy Carter created the Federal Emergency

²⁷⁹ Ilya Somin, "Federalism, the Constitution, and Sanctuary Cities," Washington Post, November 26, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/26/federalism-the-constitution-and-sanctuary-cities/?utm_term=.d8831a53e5da.

²⁸⁰ "Here's How Trump's Plan to Defund Sanctuary Cities Could Play Out," New York Daily News, November 23, 2016, <http://www.nydailynews.com/news/politics/trump-plan-defund-sanctuary-cities-play-article-1.2885423>.

Management Agency (FEMA) to improve federal emergency response in 1979.²⁸¹ The decision formalized the federal government's role in disaster response, but in 1992 this role came into question when Hurricane Andrew hit southern Florida.²⁸² Despite ample time to prepare for the storm, it took FEMA five days to arrive with supplies for survivors and first responders, which caused a national uproar.²⁸³ The failure reinvigorated qualms over the proper role for each level of government, a sentiment that was reinforced 13 years later when FEMA mismanaged its response efforts to survivors of Hurricane Katrina.²⁸⁴ These events shaped current statutes and policies, such as the Post-Katrina Emergency Management Reform Act (PKEMRA) and the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), which place state and local governments in charge of disaster response, with FEMA providing support when necessary.²⁸⁵

Today, if the federal government believes a significant storm will reach landfall in the United States, FEMA coordinates with state and local governments in the target region to open communication channels and develop a response plan but remains on standby.²⁸⁶ If the storm does hit the United States, FEMA communicates with the affected states to maintain situational awareness but does not take action until state and local resources are exhausted, and the Governor signs a disaster declaration.²⁸⁷ Once the declaration is signed and the president approves federal action, FEMA formally responds to the disaster and assists in the response and recovery efforts.²⁸⁸ This process puts state and local governments firmly in control of disaster response, leaving the federal

²⁸¹ "A Short History of FEMA," Public Broadcasting Service, November 22, 2005, <http://www.pbs.org/wgbh/pages/frontline/storm/etc/femahist.html>.

²⁸² Ibid.

²⁸³ Ibid.

²⁸⁴ Ibid.

²⁸⁵ Bruce R. Lindsay, "Stafford Act Assistance and Acts of Terrorism," Congressional Research Service, June 2, 2017, <https://fas.org/sgp/crs/homsec/R44801.pdf>.

²⁸⁶ Ibid.

²⁸⁷ Ibid.

²⁸⁸ Ibid.

government little authority to act until the affected state or states ask for federal assistance.

This is a useful model for the cyber federalism discussion, but it is too early to begin incorporating these policies because they rely on state and local governments having the capabilities necessary to handle most incidents without federal assistance. State and local first-responders have been developing and refining their capabilities for centuries, which allows them great autonomy in responding to incidents without federal government involvement. Similarly, once a state or local government develops proficient cyber capabilities, the entity is in a position to respond to cyber incidents without federal government assistance. Therefore, if state and local governments want to protect state sovereignty they should strive for the emergency management model by enhancing their current cyber capabilities.

C. APPLYING THE CONSTITUTION TO CYBER FEDERALISM

While the Constitution and supporting caselaw provide a legal framework for the balance of power among all levels of government, conflicting principles and ambiguity make it difficult to develop comprehensive cyber federalism policies. Since cybersecurity is still in its infancy as a homeland security mission, policymakers should study examples from other homeland security mission spaces for lessons learned and best practices. Therefore, this section analyzes how the homeland security missions outlined in the previous section apply the legal principles that underpin federalism and highlight concepts that can be applied to cyber federalism.

The first overarching lesson policymakers can learn from counterterrorism, immigration enforcement, and emergency management is that clear policies outlining jurisdictional boundaries improve efficiency and limit conflict. While federal and state governments have clearly defined authority in counterterrorism and emergency response, the federal government struggles to enforce immigration laws because it cannot come to an agreement with state and local governments on the proper role for each level of government. Therefore, formalizing cyber authorities for all levels of government would

strengthen the nation's ability to protect against and respond to cyber incidents as a cohesive unit.

The second lesson policymakers should take away from the other missions is that a bottom-up approach to homeland security is often more efficient and effective than a top-down approach. A bottom-up approach, whereby state and local governments lead efforts with support from the federal government, is often the most effective approach because state and local governments become force multipliers for a national strategy instead of barriers to a federal strategy. Many homeland security threats are too large for the federal government to handle alone; thus, using state and local resources makes these problems more manageable. However, the bottom-up approach requires a unified effort wherein federal, state, and local governments agree on strategies and desirable outcomes. Therefore, it is important for the federal government to work with state and local governments to determine the best policies for all partners.

A third lesson for cyber policymakers is that policies aimed at empowering state and local governments to handle homeland security issues within their jurisdictions only succeed if these governments have the required capabilities. For example, current federal emergency management policies work only because state and local governments have invested the time and resources necessary to build disaster response and mitigation capabilities. If these governments had no trained first-responders—such as law enforcement, firefighters, and emergency management services—policies empowering localized response would not be feasible. Therefore, the federal government should focus on putting state and local governments in a position to succeed in the cyber mission by providing appropriate support through money and technical expertise.

D. CONCLUSION

Overall, the federal government plays a critical role in cyber preparedness and cyber incident response, but the cyber threat environment has become too large and complex to handle alone. Instead, the nation should utilize existing legal frameworks to empower state and local governments to play a greater role in cybersecurity. Increasing the role of state and local governments would allow the federal government to focus on

large-scale threats and cyber information sharing among levels of government. Lessons learned from other homeland security missions illustrate that cyber federalism requires clearly articulated roles, improved collaboration, and increased resources to build state and local government cyber capabilities. Chapter V builds on these principles and outlines recommendations for improving cyber preparedness and incident response through cyber federalism. The remainder of this thesis identifies ways to improve the nation's cybersecurity posture while adhering to existing legal frameworks and homeland security best practices.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS AND CONCLUSION

As the nation becomes increasingly reliant on complex, interconnected information systems, the cyber risk environment expands. While the federal government should play an important role in cybersecurity, state and local governments should take more responsibility in protecting against and responding to cyber incidents. Chapter IV provided a framework for this approach by identifying three factors that are critical to federalism in other homeland security missions: (1) clearly articulating roles and responsibilities across all levels of government; (2) collaborating among all levels of government to ensure mission alignment and efficient use of resources; and (3) empowering state and local governments to handle homeland security issues through capability development. This chapter uses these guiding principles from other homeland security missions to craft recommendations for improving the nation's cybersecurity through cyber federalism.

A. RECOMMENDATION 1: IMPROVE THE LEGAL FRAMEWORKS AND JURISDICTIONAL BOUNDARIES

Cyber federalism rests on all levels of government understanding their roles in cyber preparedness and cyber incident response, but these roles are not clearly defined. Currently, one of the main factors that determines what government entity responds to a cyber incident is simply which one hears about it first. While the federal government is looking to eliminate this problem by improving federal processes through PPD-41, the directive does not address coordination between the federal government and state governments.²⁸⁹ Therefore, the continued growth of national cyber preparedness requires formal policies, a process describing the authorities of each level of government during cyber incidents, and a plan to ensure each level of government has the cyber capabilities needed to exercise their authority.

²⁸⁹ Obama, "Presidential Policy Directive – United States Cyber Incident Coordination."

1. Recommendation 1.1: Clarify Cyber Incident Responsibilities within State and Local Governments

Cyber incident response is a multifaceted process that sometimes requires parallel efforts from organizations with independent objectives. PPD-41 separates these missions into three distinct categories: threat response, asset response, and intelligence support.²⁹⁰ The directive defines threat response as “conducting appropriate law enforcement and national security investigative activity at the affected entity’s site” and defines asset response as “furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents.”²⁹¹ Intelligence support aims to improve situational awareness by coordinating information sharing and providing an integrated analysis of the cyber threat.²⁹²

It is important to clarify these distinctions because it minimizes confusion and improves efficiency during cyber incident response. For example, at the federal level, threat response is managed by the FBI because it is the lead federal law-enforcement agency while asset response is controlled by DHS because it leads cyber-related technical assistance efforts for the federal government.²⁹³ The Office of the Director of National Intelligence (ODNI) leads intelligence support activities because it is responsible for synchronizing and synthesizing intelligence across the federal government.²⁹⁴ As a result, when the federal government responds to a cyber incident, each organization understands their role, which strengthens the effectiveness of their response. States should also clarify the roles and responsibilities of their agencies during a cyber incident to ensure a coordinated and synchronized response.

²⁹⁰ Ibid.

²⁹¹ Ibid.

²⁹² Ibid.

²⁹³ Ibid.

²⁹⁴ Ibid.

2. Recommendation 1.2: Formalize Cyber Roles and Responsibilities between Levels of Government

PPD-41 is an important step toward improving the nation's cybersecurity because it details how the federal government responds to a cyber incident and which organizations have decision-making authority, but the federal government has not outlined how these responsibilities are shared with other levels of government.²⁹⁵ Therefore, Congress should formalize jurisdictional boundaries between levels of government and create a uniform cybercrime code that ensures consistency regardless of which entity handles a cyber incident.

Under the CFAA, the federal government may only prosecute cybercrimes if there is a "compelling federal interest," but this standard is ambiguous because the interconnectivity of cyber makes nearly all cybercrimes interstate in nature.²⁹⁶ Therefore, Congress must clarify these boundaries to ensure consistency and minimize redundancy. PPD-41's Cyber Incident Severity Schema provides a blueprint for a new standard by outlining the key elements for evaluating a cyber incident.²⁹⁷ These elements are "(1) the severity of the incident; (2) the urgency required for responding to a given incident; (3) the seniority level necessary for coordinating response efforts; and (4) the level of investment required of response efforts."²⁹⁸ After analyzing each of these elements, government entities can determine the scope of the incident, the resources required to address the problem, and which organization is best equipped to handle the incident based on capabilities and applicable laws.²⁹⁹

Under the PPD-41 framework, if an incident has all of these elements, it may rise to the level of a significant cyber incident.³⁰⁰ A significant cyber incident is any "cyber

²⁹⁵ Ibid.

²⁹⁶ "Prosecuting Computer Crimes."

²⁹⁷ "Cyber Incident Severity Schema," White House, accessed November 4, 2017, <https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf>.

²⁹⁸ Ibid.

²⁹⁹ For more information on the Cyber Incident Severity Schema, see Appendix.

³⁰⁰ Ibid.

incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.”³⁰¹ Based on lessons learned from other homeland security missions, multi-government incident management works best when the federal government focuses on the most complex and resource-intensive issues while state and local governments handle smaller threats. Therefore, the federal government should play a leading role in responding to significant cyber incidents because these are the incidents that are most likely to affect multiple states or impact national security.

On the other hand, states should have the lead role in cyber incidents that do not rise to the level of a significant cyber incident because they are responsible for protecting their citizens, and the Constitution empowers them to enforce their own laws.³⁰² Furthermore, each jurisdiction should prosecute cybercrimes within their territory unless the crime is part of a significant cyber incident. Since cybercrimes are borderless and malicious actors may live anywhere, prosecutorial jurisdiction should be determined by where the victim or breached system resides. If a cyber incident results in multiple victims living in multiple states, the federal government and the states should have concurrent jurisdiction. In other words, the federal government may choose to intervene, but each state should reserve the right to prosecute the malicious actors for crimes committed against victims in their jurisdiction. In all cases, all levels of government should be ready to provide incident support, even if they do not have a command role.

Another variable in determining the roles of each level of government during a cyber incident is the nexus to foreign actors. Many cyber-attacks originate from overseas, which complicates jurisdictional considerations because even a minor cyber incident may require federal government involvement. Article II of the Constitution grants the federal government authority to represent the nation in matters of foreign affairs so the federal government is best positioned to address these issues through diplomatic channels. Therefore, for legal and political reasons, the federal government should retain authority

³⁰¹ Obama, “Presidential Policy Directive – United States Cyber Incident Coordination.”

³⁰² U.S. Const. amend. X.

to prosecute foreign actors, especially if those actors were working on behalf of a foreign government.³⁰³

Admittedly, having the federal government lead all cyber cases with a foreign nexus increases the likelihood that minor cybercrimes, like Nigerian phishing scams, go unpunished, but the resources required to prosecute these crimes are immense, and the probabilities of tracking down each scammer are low. Instead, the federal government should work with other levels of government and other countries to increase public awareness of these scams and to ensure these countries are prosecuting their citizens for these crimes. While these steps will not prevent all cyber-attacks from foreign actors, they will decrease the likelihood of these attacks being successful and make future attacks less appealing for criminals.

3. Recommendation 1.3: Strengthen Cybercrime Prosecution by Standardizing Cyber Laws

One of the first steps for improving consistency in cyber incident response is developing comprehensive cybercrime legislation that standardizes how these crimes are defined and enforced. Currently, states statutes expressly prohibit certain cybercrimes, while other cybercrimes are not expressly prohibited so they are prosecuted through traditional criminal laws.³⁰⁴ For example, only California and Wyoming have legislation that addresses ransomware while all other states use existing extortion or computer trespass laws to prosecute these offenders.³⁰⁵ The deficiencies in cybercrime legislation makes it difficult to clarify jurisdictional boundaries because each entity defines and punishes the crime differently. Therefore, increased uniformity in cybercrime laws would stabilize these boundaries.

These uniform standards must incorporate basic criminal law principles—that is, the intent of the actor (*mens rea*), the act committed (*actus reus*), and harm to the victim

³⁰³ U.S. Const. art. II.

³⁰⁴ Pam Greenburg, “Computer Crime Statutes,” National Conference of State Legislators, December 5, 2016, <http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx>.

³⁰⁵ Ibid.

(causation)—to classify cybercrimes. *Mens rea* is important because the law should only punish those intending to cause harm, not those who cause harm by accident. *Actus reus* is also important because a guilty mind should only be punished if the person follows through on those thoughts. Finally, causation is critical because the government must show that the actions caused the intended harm, or a reasonable person could have expected that these actions would cause harm.

Once states have cybercrimes clearly defined in their penal codes, the nation must agree on standardized cybercrime classifications, such as a minimum standard for misdemeanor cybercrimes and felony cybercrimes. In the CFAA, a cybercrime rises to the level of a felony if the value of damage exceeds \$5,000, but it can be difficult to measure the financial harm of some cybercrimes.³⁰⁶ For example, this threshold does not account for cybercrimes with psychological or emotional harm, such as cyberstalking or cyberbullying, because these crimes do not have intrinsic dollar values. Therefore, any comprehensive penal code for cybercrimes must account for cybercrime's evolution since the CFAA was enacted in 1986.³⁰⁷

Instead of basing cybercrime classifications solely on fiscal damage, a comprehensive penal code for cybercrimes should punish cybercrimes based on the totality of the consequences, which include profits accrued as well as digital, physical, or psychological damage caused by the crime. A uniform cybercrime standard should also ensure that malicious actors are punished in proportion to the consequences of their crimes. For example, it would be a misdemeanor for an individual to access a computer intentionally without authorization even if the assailant caused no damage and did not profit from the data on the computer. However, it would be a felony if the malicious actor stole proprietary data from the computer and sold the information to a third party for \$500,000. Similarly, it might be a felony if the malicious actor stole embarrassing photos from the computer and used these photos to cause serious, irreparable psychological harm. Overall, the precise threshold for when a misdemeanor becomes a felony must be

³⁰⁶ Grant Burningham, "The Most Hated Law on the Internet and its Many Problems," *Newsweek*, April 16, 2016, <http://www.newsweek.com/most-hated-law-internet-and-its-many-problems-cfaa-448567>.

³⁰⁷ Andrew Coutts, "You're Probably Unknowingly Breaking Laws Online Thanks to the CFAA," *Digital Trends*, January 17, 2013, <https://www.digitaltrends.com/web/understanding-the-cfaa/>.

left up to each individual state in accordance with the 10th Amendment, but each state should adhere to the same basic principles of proportionality in their sentencing.

In some cases, if a cybercrime causes enough damage, such as loss of life, a proportional sentence may be capital punishment. For example, if a ransomware attack on a hospital prevents patients from receiving appropriate medical care and a patient dies because of this delay in treatment, the attack should be seen as homicide and the perpetrator should be punished in accordance with the homicide laws of that jurisdiction. The CFAA states, “If the offender attempts to cause or knowingly or recklessly causes death,” the maximum sentence is life imprisonment.³⁰⁸ The United Kingdom can also sentence criminals to life in prison if their cyber-attack causes death.³⁰⁹ However, some countries, such as Nigeria, have increased the maximum sentence for certain cybercrimes to capital punishment if the cyber-attack is deadly.³¹⁰ While capital punishment laws differ from state to state, all levels of government should examine current cybercrime sentences and ensure that these punishments fit the crime, especially for felony cybercrimes in which the cyber-attack results in death.

On the other end of the spectrum, some cybercrimes appear to be a mere public nuisance that cause minimal damage, such as spam emails, but even these crimes can cause harm to consumers and companies.³¹¹ For example, a spam email may expose consumers—including underage consumers—to inappropriate or offensive content and may contain links that upload malware onto a user’s system, which can cause harm to a computer and the user. Additionally, spam emails monopolize bandwidth at the expense of Internet service providers and email services, which increases costs and limits processing power.³¹² Therefore, these unsolicited emails should be controlled and the

³⁰⁸ *Computer Fraud and Abuse Act*, 18 U.S. Code 47 § 1030 (c)(4)(F).

³⁰⁹ Thomas Fox-Brewster, “UK Introduced Life Sentences for Killer Hackers This Month. In Nigeria, it’s the Death Penalty,” *Forbes*, May 13, 2015, <https://www.forbes.com/sites/thomasbrewster/2015/05/13/death-penalty-or-life-for-hackers/#7f1bb1306464>.

³¹⁰ *Ibid.*

³¹¹ Grant Gross, “Is the CAN-SPAM Law Working?” *PC World*, January 13, 2004, <https://www.pcworld.com/article/114287/article.html>.

³¹² *Ibid.*

malicious actors should be held accountable. These minor offenses should be considered misdemeanor cybercrimes and regulated through heavy fines, much like unsolicited telemarketer phone calls.³¹³

If the United States wants to lower the frequency and severity of cybercrimes, it must create a legal framework that enables prosecutors to pursue justice for all kinds of cybercrimes, whether minor or severe. It would be impossible to legislate each kind of cybercrime and their consequences; therefore, the nation needs a penal structure that is flexible enough to incorporate all cybercrimes yet precise enough to enforce. Table 1 creates the confines for this structure by grouping all cybercrimes into two major categories, misdemeanors and felonies, and describing the kinds of cybercrimes that fit into these categories. Felonies are further broken down to highlight the crimes that are serious enough to be considered a capital offense.

Table 1. Proposed Cybercrimes Classifications and Sentencing Guidelines.

Classification		Crime Committed	Punishment
Felony	A and B	Serious offenses resulting in death or serious bodily injury, including but not limited to <ul style="list-style-type: none"> • Large-scale attack on power grid • Hate crimes 	Minimum of 25 years to life in prison, including death penalty. Up to a \$250,000 fine.
	C, D, and E	Serious offenses, including but not limited to <ul style="list-style-type: none"> • Computer fraud • Child pornography 	One year to 25 years in prison. Up to a \$250,000 fine.
Misdemeanor		Minor offenses, including but not limited to <ul style="list-style-type: none"> • Email spamming • Phishing • Cyber bullying 	Less than one year in prison. Up to a \$100,000 fine.

The table summarizes what constitutes a misdemeanor and felony, including capital offenses, based on the recommendations outlined in this section and the United

³¹³ “The Telemarketing Sales Rule,” Federal Trade Commission, accessed November 4, 2017, <https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule>.

States Penal Code.³¹⁴ Notably, the specific crimes listed may require a higher classification if the physical, financial, or psychological damage warrants a more severe punishment. Overall, the chart is designed to provide a framework for future discussions and to help legislators understand how cybercrimes fit within current sentencing structures.

Moving forward, all levels of government must strengthen their cybercrime laws and clearly define cybercrime classifications. Additionally, the federal government must simplify the “compelling federal interest” standard by reserving the right to prosecute all crimes that violate federal statutes, but focusing resources on serious felonies that stem from a significant cyber incident.³¹⁵ On the other hand, states should retain authority to prosecute all misdemeanor crimes and felony acts that do not violate federal law or the federal government chooses not to pursue. By empowering the states with this authority, it allows the federal government to focus on the most serious and complex cases while also ensuring the integrity of the cyber federalism construct. It also encourages states to improve their cybercrime statutes and allows them to protect their citizens with the laws that best fit the needs of their jurisdiction.

B. RECOMMENDATION 2: INCREASE CYBER INVESTMENTS AND MAXIMIZE EXISTING RESOURCES

While the number of cyber incidents continues to grow each year, state and local governments rarely make cybersecurity a funding priority.³¹⁶ In 2015, the Ponemon Institute estimated that half of state and local governments experienced six to 25 cyberattacks in the previous 24 months, but most state budgets allocate less than two-percent of their information security funding on cybersecurity.³¹⁷ If state and local governments are serious about securing their digital infrastructure from a growing cyber threat, they need to increase their cybersecurity investments and maximize existing resources.

³¹⁴ *Violent Crime Control and Law Enforcement Act*, 18 U.S. Code 227 § 3559.

³¹⁵ “Prosecuting Computer Crimes.”

³¹⁶ Greg Garcia, “A Look at State and Local Cybersecurity Funding,” Signals Group DC, December 7, 2016, <https://signalgroupdc.com/policyber-state-cybersecurity-funding/>.

³¹⁷ *Ibid.*

1. Recommendation 2.1: Prioritize Cybersecurity in Future Budgets and Create a Federal Cyber Grant Program

Since the terrorist attacks of September 11, 2001, foreign-born terrorism has attributed for roughly six deaths in America each year and the United States has spent over \$100 billion per year to deter or disrupt acts of terrorism during that timeframe.³¹⁸ While some may argue that the money spent on counterterrorism is the reason for the small number of terrorism-related deaths each year, the dollar amount speaks to the larger issue of prioritization. Over 80 percent of state CIOs believe that a lack of funding is their number one barrier to addressing cybersecurity gaps, which suggests that even when state and local governments have the money to spend on security, they do not invest these resources in cybersecurity.³¹⁹ Moving forward, states must reevaluate this strategy because recent cyber-attacks to critical infrastructure, such as power grids and election systems, and other public services demonstrate the potential impacts of future incidents and highlight the importance of making cybersecurity a priority.³²⁰

Federal preparedness grant programs also need to make cybersecurity a priority. From 2011 to 2014, FEMA's HSGP program awarded states over four-billion dollars to address capability gaps, but states spent a total of \$27.3 million on cybersecurity.³²¹ In fiscal year 2016 alone, FEMA awarded state and local governments \$1,617,000,000 to build capabilities in terrorism prevention, port security, and various forms of transit security, but none of this funding was specifically allocated for cybersecurity.³²² While cybersecurity is an "allowable expense" under the HSGP, there are no specific grants for

³¹⁸ Dave Mosher and Skye Gould, "How Likely are Foreign Terrorists to Kill Americans? The Odds May Surprise You," Business Insider, January 31, 2017, <http://www.businessinsider.com/death-risk-statistics-terrorism-disease-accidents-2017-1>.

³¹⁹ 2016 Deloitte-NASCIO Cybersecurity Study.

³²⁰ Ellen Nakashima, "Russia has Developed a Cyberweapon that can Disrupt Power Grids, According to New Research," Washington Post, June 12, 2017, https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html?utm_term=.443461daea9c.

³²¹ Garcia, "A Look at State and Local Cybersecurity Funding."

³²² "Grant Program Directorate Information Bulletin No. 411a."

cybersecurity, which means states do not have to spend their grant money on improving their cybersecurity.³²³

Conversely, Section 2006 of the Homeland Security Act of 2002 requires states to spend at least 25 percent of HSGP funds on terrorism prevention activities.³²⁴ In addition, last year FEMA awarded \$10 million in Countering Violent Extremism grants, \$10 million in tribal grants to prevent terrorism and \$39 million in Complex Coordinated Attack grants.³²⁵ Simply put, the disparity between counterterrorism grant funding and cybersecurity grant funding is a problem.

Recently, Representative Derek Kilmer of Washington introduced a bill, entitled the State Cyber Resiliency Act, which addresses this problem by creating a preparedness grant program specifically for cybersecurity.³²⁶ The program would provide funding to states so they can develop their cyber capabilities by adopting cybersecurity best practices, addressing cyber workforce gaps, improving digital infrastructure, and establishing scholarships and apprenticeships to improve cyber education.³²⁷ This program would be a significant step for the nation as it works together to improve cyber resiliency across all levels of government.

2. Recommendation 2.2: Enhance Threat Detection and Indicator Sharing through State-led Cyber Operation Centers and/or by Expanding the Roles and Capabilities of Fusion Centers

Cyber information sharing can be resource intensive as it requires money and personnel to gather, verify and share information with counterparts across the field.³²⁸ However, if managed properly, the long-term benefits outweigh initial costs and

³²³ Garcia, “A Look at State and Local Cybersecurity Funding.”

³²⁴ Ibid.

³²⁵ Ibid.

³²⁶ “H.R. 1344 – State Cyber Resiliency Act,” Congress, accessed November 4, 2017, <https://www.congress.gov/bill/115th-congress/house-bill/1344>.

³²⁷ Ibid.

³²⁸ Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka, “Guide to Cyber Threat Information Sharing,” NIST Special Publication, October 2016, page 5, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>.

minimize future costs because the information allows partners to have greater understanding of their threats and to be more efficient in addressing these threats.³²⁹ Therefore, each state and large municipality should have at least one cyber operations center that allows them to share information across their state and with other information sharing hubs across the nation.

States should also look to repurpose, or expand the mission requirements of, existing operation centers that have the infrastructure for information sharing. For example, fusion centers were designed to facilitate information sharing on terrorism, but some fusion centers are expanding their mission to include cyber threat information sharing.³³⁰ This allows states to utilize existing resources to address cybersecurity without wasting time and money on new facilities and new equipment. Therefore, each state should look to expand the role of their fusion centers to include cyber threat information sharing, thereby utilizing existing resources, processes, and relationships of fusion centers to streamline cyber threat information sharing initiatives.

3. Recommendation 2.3: Create an Agile Cyber Workforce with the Ability to Expand during a Cyber Incident

Given the difficulties that state and local governments have in developing their cyber workforce, it is unrealistic to assume they will have the personnel needed to respond to all incidents. Instead, states need a scalable workforce that is able to handle day-to-day cybersecurity but also able to expand quickly if a cyber incident overwhelms local personnel. Therefore, states should develop a cyber reservist cadre that activates during large cyber incidents to support local response teams. These cyber reservists can be from the National Guard or even volunteer cyber responders, much like the volunteer firefighters that many jurisdictions use around the country.

³²⁹ Ibid.

³³⁰ Brian Nussbaum, "State and Local Cyber Security: The Rapid Growth of Cyber in Fusion Centers," Stanford University Center for Internet and Society, March 15, 2016, <http://cyberlaw.stanford.edu/blog/2016/03/state-and-local-cyber-security-rapid-growth-cyber-fusion-centers>.

State and local entities should also explore opportunities for mutual aid agreements with other jurisdictions because it allows organizations to address capability gaps without investing new resources. In fact, cyber's global reach strengthens the utility of mutual aid agreements because state and local governments are not limited to bordering territories. Governments can enter into agreements with any jurisdiction in the country, which means the opportunities for collaboration are limitless. Therefore, state and local governments should work together and share resources, especially in an environment where the threat is growing and resources are scarce.

4. Recommendation 2.4: Create “Cyber 9-1-1” to Centralize Cyber Incident Reporting

If state and local governments are going to take a larger role in the cybersecurity mission, there must be greater consistency in how they handle cyber incidents and how victims notify the government of cyber incidents. The federal government has simplified cyber incident reporting by implementing a “just tell someone” policy where victims can contact any federal agency with cyber responsibilities and putting the burden on the agencies to determine jurisdiction.³³¹ This makes it easier for victims to inform the federal government of ongoing attacks and prevents them from wasting time trying to search for the proper federal agency to contact, which gives incident responders more time to address the threat and mitigate consequences.

States should take this one step further by developing their own “Cyber 9-1-1” reporting tool that allows victims to call or email one central location that assesses reports and routes each report accordingly. This would help government entities coordinate their response efforts and make it easier for victims to know who to contact during a cyber emergency. Additionally, states should look for ways to automate assessments of incident reports to maximize efficiency and preserve resources.

³³¹ “Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government,” DHS, accessed November 4, 2017, <https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf>.

C. RECOMMENDATION 3: EMPHASIZE CYBER EDUCATION AND COLLABORATION AMONG THE PUBLIC SECTOR, PRIVATE SECTOR, AND ACADEMIA

As the cyber workforce gap expands, it amplifies the need for a multilayered cyber education and training strategy at the state and local level. These governments need to work with schools and universities to develop a cyber education pathway that begins in grade schools and continues into high schools and colleges as required courses for graduation. High schools and colleges should identify gifted students and place them in advanced programs to nurture their talents, much like the advanced trainings offered to promising young athletes and musicians. This strategy would help develop the current workforce, but also position the nation for growing cyber demands in the future.

1. Recommendation 3.1: Incorporate Cyber Education in School Curriculums for Children of All Ages

According to the nonprofit organization Change the Equation, 22 percent of 12th graders in the United States have taken at least one computer programming class in their life.³³² Moreover, less than half of the 12th graders in the United States have access to a computer science class.³³³ These are troublesome statistics, but state and local governments are in the best position to alter these trends because they set the guidelines for grade school and high school curriculums.

Moving forward, the Department of Education should encourage schools to incorporate cybersecurity classes in middle school and high school curriculums, and develop grant programs to ensure that schools have the resources to offer these classes. State and local governments should explore ways to increase the number of cybersecurity and computer science classes for middle school and high school students, and consider mandating these classes as part of statewide curriculums. Schools should also explore aligning cybersecurity and computer science classes with their language departments so children have the option to take these classes in lieu of traditional language classes, such

³³² “New Data: Bridging the Computer Science Access Gap,” Change the Equation, August 9, 2016, <http://changetheequation.org/blog/new-data-bridging-computer-science-access-gap-0>.

³³³ Ibid.

as Spanish or Latin. Additionally, states should work with their National Guard and federal government counterparts to bring cyber experts into classrooms for specialized training and recruiting, especially in underprivileged areas where resources make it more difficult to identify and cultivate talented students.

2. Recommendation 3.2: Place Greater Emphasis on Computer Science Programs in Universities

As described in Chapter III, some states are working to improve cyber education and training at the college level, but few college curriculums are adapting to the growing needs.³³⁴ A recent survey of the top computer science programs in the United States found that none of the top 10 universities require a cybersecurity course to graduate and only three in the top 50 require at least one cybersecurity course.³³⁵ This suggests that the nation's universities do not see cybersecurity as a priority class and have not yet developed the programmatic infrastructure needed to improve cyber education.

Moving forward, universities must look to offer more computer science classes, but particularly cybersecurity classes, and explore ways to incorporate cybersecurity education in non-computer science degree programs as cybersecurity should be integrated into every field of study. State and local governments should expand their scholarship and grant programs for cybersecurity studies, particularly for students that agree to work for in the public sector after they graduate.

3. Recommendation 3.3: Develop Technology Parks that Bring the Public Sector, Private Sector, and Academia to a Central Location

One of the best examples of integrating leaders in technology from the public sector, the private sector, and academia is Stanford's relationship with its neighbors in Silicon Valley. Silicon Valley is widely seen as a world leader in technology and many of their most notable residents—such as the leaders for Hewlett-Packard, Google, and

³³⁴ Sarah K. White, "Top U.S. Universities Failing at Cybersecurity Education," CIO.com, April 25, 2016, <http://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html>.

³³⁵ Ibid.

Yahoo—come from Stanford.³³⁶ In fact, over 50 percent of Silicon Valley’s products come from Stanford alumni.³³⁷

Other countries, such as Israel, are trying to recreate Silicon Valley’s relationship with Stanford by creating technology parks, such as the Advanced Technology Park and CyberSpark, which co-locate members of the cyber community to maximize resources and simplify collaboration.³³⁸ These parks offer state-of-the-art cyber facilities that allow the cyber community to train, educate, research, and develop together with the best equipment and the brightest cyber minds.³³⁹ This proactive approach to cross-sector collaboration has been very successful as Israel owns one of the stronger cyber armies in the world and their cybersecurity firms own roughly 10 percent of an \$11.9 billion global cyber market.³⁴⁰

Moving forward, state and local governments should strive to recreate Stanford’s symbiotic relationship with Silicon Valley by incentivizing collaboration through technology parks or similar programs. These programs provide research facilities for local universities, government entities, and the private sector to explore and innovate in a collaborative environment. Increased collaboration would not only improve relationships in the community and promote innovation, but also incentivize companies from around the world to come to their state, which would create new jobs and new opportunities for economic growth.

D. CONCLUSION

In conclusion, America’s infrastructure relies on interconnected and interdependent information systems, which fuel productivity, efficiency and prosperity,

³³⁶ “History of Stanford,” Stanford University, accessed November 4, 2017, https://www.stanford.edu/about/history/history_ch3.html.

³³⁷ Hamilton, “Scholar Examines Links between Stanford, Silicon Valley.”

³³⁸ Niv Elis, “Netanyahu Declares Beersheba Cyber Security Hub,” Jerusalem Post, January 27, 2014, <http://www.jpost.com/Business/Business-News/Netanyahu-declares-Beersheba-Cyber-Security-hub-339539>.

³³⁹ Ibid.

³⁴⁰ Andrew Zaleski, “The Latest Hot Start-ups to Emerge from Israel’s Cybersecurity War Machine,” CNBC, February 28, 2017, <http://www.cnbc.com/2017/02/28/the-latest-hot-start-ups-to-emerge-from-israels-cybersecurity-war-machine.html>.

but also creates a cyber threat environment that is too complex for the federal government to handle alone. The federal government is a driving force in national security, but state and local governments must play a critical role in cybersecurity by developing the cyber capabilities necessary to protect against and respond to cyber incidents. After all, while the United States has evolved from 13 loosely organized states into the most powerful nation in the world, its federalist roots remain a defining element of its governing structure and as the nation progresses through the digital age, these ideals must extend into the cyber realm.

State and local governments may be best positioned to handle many cyber incidents, but many of these entities do not have the policies, resources, and capabilities required to protect against and respond to cyber incidents. Therefore, the nation should focus on strengthening state and local cyber capabilities so these entities can address localized threats, thereby allowing the federal government to focus its resources on large-scale information sharing, significant cyber incidents, and international matters. The nation must also clarify jurisdictional boundaries between all levels of government and improve legal standards so laws are enforced consistently across the country. Table 2 outlines the three recommendations for improving cyber federalism and the tasks for implementing these recommendations.

Table 2. Overview of Recommendations.

Recommendations	Steps for Implementation
Improve the legal frameworks that shape cybersecurity by formalizing jurisdictional boundaries and standardizing cybercrime laws.	Clarify cyber incident responsibilities within state and local governments
	Formalize cyber roles and responsibilities between levels of government.
	Standardize cybercrime statutes.
Strengthen state and local cyber incident response capabilities by increasing financial investments and maximizing existing resources.	Prioritize cybersecurity spending.
	Enhance state-led cyber operation centers.
	Create a malleable cyber workforce.
	Create “Cyber 9-1-1.”
Expand cyber workforce by increasing emphasis on cyber education and collaboration between the public sector, private sector, and academia.	Improve cyber education.
	Emphasize computer science programs.
	Develop technology parks.

If the nation wants to maintain its reputation as a world leader in the cyber community and improve its cyber posture, it must embrace a bottom-up approach that empowers state and local governments to play a larger role in cybersecurity. Cyber federalism would make the nation more adaptable and dynamic when protecting against rapidly evolving cyber threats, which would improve cybersecurity for the nation as a whole. Overall, the key to success against America's newest threat lies in one of its oldest traditions so it is time for the nation to embrace its past as it prepares for the future.

APPENDIX. CYBER INCIDENT SEVERITY SCHEMA

In 2016, President Barack Obama released *Presidential Policy Directive (PPD) 41: United States Cyber Incident Coordination*, to improve cyber incident response coordination within the federal government.³⁴¹ Alongside PPD-41, President Obama released the Cyber Incident Severity Schema, which provides a rubric for analyzing cyber incidents and determining the proper level of federal response.³⁴² Table 3 recreates the Cyber Incident Severity Schema, including the colors associated with each level. It also demarcates the threshold where a cyber incident rises to significant cyber incident.³⁴³

Table 3. PPD-41 Cyber Incident Severity Schema.

Incident Level		General Definition
Significant Cyber Incident	Level 5 Emergency (Black)	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons
	Level 4 Severe (Red)	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
	Level 3 High (Orange)	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Cyber Incident	Level 2 Medium (Yellow)	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
	Level 1 Low (Green)	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
	Level 0	Unsubstantiated or inconsequential event.

³⁴¹ Obama, “Presidential Policy Directive – United States Cyber Incident Coordination.”

³⁴² “Cyber Incident Severity Schema.”

³⁴³ Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Accenture Consulting. *Cyber Threats Facing State and Local Government*. 2016.
https://www.accenture.com/t20170203T030414__w__/us-en/_acnmedia/PDF-41/Accenture-NASCIO-Cyber-POV-v02.pdf.
- Anderson, Nate. "Confirmed: US and Israel Created Stuxnet, Lost Control of it." *Ars Technica*. June 1, 2012. <https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/>.
- Antiterrorism Act*. 18 U.S. Code 113B § 2332a.
- . 18 U.S. Code 113B § 2332b.
- Armacost, Barbara E. "'Sanctuary' Laws: The New Immigration Federalism." *Michigan State Law Review*. 2016.
https://static1.squarespace.com/static/55549704e4b0565df9f2305b/t/5899e9ea9de4bb90ccdae372/1486481898620/01_Armacost_Soft+Edits.pdf.
- Barnett, Randy. "The Choice between Madison and FDR." *Georgetown University Law Center*. 2008.
<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1840&context=facpub>
- Blake, Andrew. "Pennsylvania Endured 90 Billion Attempted Cyber Intrusions in 2017: Report." *Washington Times*. July 18, 2017.
<http://www.washingtontimes.com/news/2017/jul/18/pennsylvania-suffered-90-billion-attempted-cyberat/>.
- Bo Williams, Katie. "DHS Designates Election Systems as 'Critical Infrastructure'." *The Hill*. January 6, 2017. <http://thehill.com/policy/national-security/313132-dhs-designates-election-systems-as-critical-infrastructure>.
- British Broadcasting Corporation. "Freddie Gray's Death in Police Custody – What we Know." May 23, 2016. <http://www.bbc.com/news/world-us-canada-32400497>.
- Brunacini, Nick. "NIMS or NIIMS." *Fire Rescue Magazine*. July 30, 2009.
<http://www.firerescuemagazine.com/articles/print/volume-1/issue-3/command-leadership/nims-or-niims.html>.
- Burningham, Grant. "The Most Hated Law on the Internet and its Many Problems." *Newsweek*. April 16, 2016. <http://www.newsweek.com/most-hated-law-internet-and-its-many-problems-cfaa-448567>.

- Business Insider. "National Retail Federation Estimates 8-12% US E-commerce Growth in 2017." February 10, 2017. <http://www.businessinsider.com/national-retail-federation-estimates-8-12-us-e-commerce-growth-in-2017-2017-2>.
- Business Pundit. "10 Most Costly Cyber Attacks in History." August 15, 2011. <http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history/>.
- California Department of Justice. "California Cyber Crime Center." Accessed November 4, 2017. <https://oag.ca.gov/c4>.
- Carafano, James and Richard Weitz. "Learning from Disaster: The Role of Federalism and the Importance of Grassroots Response." The Heritage Foundation. March 21, 2006. <http://www.heritage.org/homeland-security/report/learning-disaster-the-role-federalism-and-the-importance-grassroots>.
- CBS Baltimore. "New Documents Show Cyber Hackers Struck Baltimore Days after Riots." July 31, 2015. <http://baltimore.cbslocal.com/2015/07/31/new-documents-show-cyber-hackers-struck-baltimore-after-riots/>.
- CBS News. "Law Enforcement Says Yahoo Account Hacks were Likely Sponsored by Foreign Government." December 15, 2016. <http://www.cbsnews.com/news/yahoo-hack-law-enforcement-believes-state-actor-us-official-says/>.
- Chacon, Jennifer. "Who is Responsible for U.S. Immigration Policy?" American Bar Association. Accessed November 4, 2017. https://www.americanbar.org/publications/insights_on_law_and_society/14/spring-2014/who-is-responsible-for-u-s--immigration-policy-.html.
- Change the Equation. "New Data: Bridging the Computer Science Access Gap." August 9, 2016. <http://changetheequation.org/blog/new-data-bridging-computer-science-access-gap-0>.
- Cisco. "What Is the Difference: Viruses, Worms, Trojans, and Bots?" Accessed November 4, 2017. <http://www.cisco.com/c/en/us/about/security-center/virus-differences.html>.
- Clapper, James. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community." Office of the Director of National Intelligence. February 9, 2016. https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FIN_AL.pdf.
- Clay, Kelly. "Washington State Courts Hacked: 160,000 Social Security Numbers Potentially Accessed." Forbes. May 10, 2013. <https://www.forbes.com/sites/kellyclay/2013/05/10/washington-state-courts-hacked-160000-social-security-numbers-potentially-accessed/#7f71701636fa>.

- Coats, Daniel. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community." Senate Select Committee on Intelligence. May 11, 2017.
<https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf>.
- Computer Fraud and Abuse Act*. 18 U.S. Code 47 § 1030 (c)(4)(F).
- Computer History Museum. "Timeline of Computer History." Accessed November 4, 2017. <http://www.computerhistory.org/timeline/1961/>.
- Congress. "H.R. 1344 – State Cyber Resiliency Act." Accessed November 4, 2017.
<https://www.congress.gov/bill/115th-congress/house-bill/1344>.
- Congressional Resources. "About the Federalist Papers." Accessed November 4, 2017.
<https://www.congress.gov/resources/display/content/About+the+Federalist+Papers>.
- Couts, Andrew. "You're Probably Unknowingly Breaking Laws Online Thanks to the CFAA." Digital Trends. January 17, 2013.
<https://www.digitaltrends.com/web/understanding-the-cfaa/>.
- Daniel, Michael. "State and Local Government Cybersecurity." White House Archives. April 2, 2014. <https://obamawhitehouse.archives.gov/blog/2014/04/02/state-and-local-government-cybersecurity>.
- Daniels, Lisa. "Prosecuting Terrorism in State Court." Lawfare Blog. October 26, 2016.
<https://www.lawfareblog.com/prosecuting-terrorism-state-court>.
- Davies, Alex. "Detroit is Stomping Silicon Valley in the Self-driving Car Race." Wired. April 3, 2017. <https://www.wired.com/2017/04/detroit-stomping-silicon-valley-self-driving-car-race/>.
- Dawson, Gregory and Kevin C. Desouza. "How State Governments are Addressing Cybersecurity." Brookings Institute. March 5, 2015.
<https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/>.
- Department of Commerce. "U.S. Census Bureau News." May 16, 2017.
https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.
- Department of Homeland Security. "Critical Infrastructure Sector Partnerships." Accessed November 4, 2017. <https://www.dhs.gov/critical-infrastructure-sector-partnerships>.

- . “Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government.” Accessed November 4, 2017.
<https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf>.
- . “Information Sharing and Analysis Organizations (ISAOs).” Accessed November 4, 2017. <https://www.dhs.gov/isao>.
- . “Information Sharing.” Accessed November 4, 2017.
<https://www.dhs.gov/topic/cybersecurity-information-sharing>.
- . “National Cyber Incident Response Plan.” US-CERT. December 2016.
https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.
- . “National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience.” Accessed November 4, 2017.
https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf
- . “National Network of Fusion Centers Fact Sheet.” Accessed November 4, 2017.
<https://www.dhs.gov/national-network-fusion-centers-fact-sheet>.

Department of Justice. “Baseline Capabilities for State and Major Urban Area Fusion Centers.” Justice Information Sharing. September 2008.
<https://it.ojp.gov/documents/d/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf>.

Department of Transportation. “Smart City Challenge.” Accessed November 4, 2017.
<https://www.transportation.gov/sites/dot.gov/files/docs/Smart%20City%20Challenge%20Lessons%20Learned.pdf>.

Drummond, David. “New Approach to China.” Google Official Blog. January 12, 2010.
<https://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.

Duncan, Ian. “City Faced Cyberattacks amid Chaos and Unrest on the Streets.” Baltimore Sun. July 31, 2015. <http://www.baltimoresun.com/news/maryland/sun-investigates/bs-md-ci-cyber-riot-20150731-story.html>.

Eidam, Eyragon. “New Jersey Takes Consolidated, Fusion Center-Style Approach to Cybersecurity.” Gov Tech. April 29, 2016.
<http://www.govtech.com/security/New-Jersey-Takes-Consolidated-Fusion-Center-Style-Approach-to-Cybersecurity.html>.

Elis, Niv. “Netanyahu Declares Beersheba Cyber Security Hub.” Jerusalem Post. January 27, 2014. <http://www.jpost.com/Business/Business-News/Netanyahu-declares-Beersheba-Cyber-Security-hub-339539>.

- Eunjung Cha, Ariana and Ellen Nakashima. "Google China Cyberattack Part of a Vast Espionage Campaign, Experts Say." Washington Post. January 14, 2010. <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html>.
- Federal Computer Week. "State of Cybersecurity in Local, State and Federal Government." Accessed November 4, 2017. <https://fcw.com/pages/hpsp/hpsp-10.aspx>.
- Federal Emergency Management Agency. "Grant Program Directorate Information Bulletin No. 411a." November 30, 2016. https://www.fema.gov/media-library-data/1482424650311-62d42ea5e0fd5f392d819372ba003496/FY16_Prep_Grant_Allocations_IB411a_GPD_Approved_v508.pdf.
- . "National Incident Management System." December 2008. https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.
- . "National Preparedness Goal." September 2015. https://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf.
- . "National Preparedness Report." March 30, 2016. https://www.fema.gov/media-library-data/1476817353589-987d6a58e2eb124ac6b19ef1f7c9a77d/2016NPR_508c_052716_1600_alla.pdf.
- . "National Preparedness System." November 2011. https://www.fema.gov/media-library-data/20130726-1855-25045-8110/national_preparedness_system_final.pdf.
- . "NIMS: Frequently Asked Questions." Accessed November 4, 2017. <https://www.fema.gov/pdf/emergency/nims/nimsfaqs.pdf>.
- . "Preparedness (Non-Disaster) Grants." Accessed November 4, 2017. <https://www.fema.gov/preparedness-non-disaster-grants>.
- Federal Trade Commission. "The Telemarketing Sales Rule." Accessed November 4, 2017. <https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule>.
- Finklea, Kristin. "The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement." Congressional Research Service. January 17, 2013. <https://fas.org/sgp/crs/misc/R41927.pdf>.
- Finklea, Kristin and Catherine A. Theohary. "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement." Congressional Research Service. January 15, 2015. <https://fas.org/sgp/crs/misc/R42547.pdf>.

- Fire Eye. "What is a Zero-Day Exploit?" Accessed November 4, 2017.
<https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html>.
- Fox-Brewster, Thomas. "UK Introduced Life Sentences for Killer Hackers This Month. In Nigeria, it's the Death Penalty." *Forbes*. May 13, 2015.
<https://www.forbes.com/sites/thomasbrewster/2015/05/13/death-penalty-or-life-for-hackers/#7f1bb1306464>.
- Garcia, Greg. "A Look at State and Local Cybersecurity Funding." Signals Group DC. December 7, 2016. <https://signalgroupdc.com/policyber-state-cybersecurity-funding/>.
- Giaimo, Cara. "In 1988, One Rogue Worm Shut Down 10 Percent of the Internet." *Atlas Obscura*. November 3, 2015. <http://www.atlasobscura.com/articles/in-1988-one-rogue-worm-shut-down-10-percent-of-the-internet>.
- Gibbons v. Ogden*. 22 U.S. 1. 1824.
- Glennon, Michael J. "State-Level Cybersecurity." Hoover Institute at Stanford University. February 1, 2012.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997565.
- Greenburg, Pam. "Computer Crime Statutes." National Conference of State Legislators. December 5, 2016. <http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx>.
- Gross, Grant. "Is the CAN-SPAM Law Working?" *PC World*. January 13, 2004.
<https://www.pcworld.com/article/114287/article.html>.
- Hall, Gina. "How Detroit Automakers are Trying to Lure Away Silicon Valley Tech Talent." *Silicon Valley Business Journal*. May 9, 2017.
<https://www.bizjournals.com/sanjose/news/2017/05/09/ford-gm-detroit-tech-hiring-silicon-valley-waymo.html>.
- Hamilton, Alexander. "Federalist Number 67." Congressional Resources. 1787.
<https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-67>.
- . "Federalist Number 9." Congressional Resources. 1787.
<https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-9>.
- Hamilton, Andrea M. "Scholar Examines Links between Stanford, Silicon Valley." Stanford University. April 16, 2003.
<http://news.stanford.edu/news/2003/april16/historysusv-416.html>.

- Hathaway, Melissa. *Cyber Readiness Index 2.0*. Potomac Institute for Policy Studies. November 2015.
<http://www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-index-2.0-web-2016.pdf>.
- Indiana. "Indiana Cybersecurity." Accessed November 4, 2017.
<http://www.in.gov/cybersecurity/2402.htm>.
- InfraGard. "More Information." Accessed November 4, 2017.
<https://www.infragard.org/Application/General/MoreInfo>.
- Johnson, Chris, Lee Badger, David Waltermire, Julie Snyder, and Clem Skorupka. "Guide to Cyber Threat Information Sharing." NIST Special Publication. October 2016. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>.
- Johnson, Jeh. "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." DHS. January 6, 2017.
<https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.
- Kerr, Dara. "Ferguson, Mo., Police Site Hit with DDoS Attack." CNET. August 14, 2014. <https://www.cnet.com/news/st-louis-police-website-suffers-ddos-attack/>.
- Kleinbard, David and Richard Richtmyer. "U.S. Catches 'Love' Virus." May 5, 2000.
<http://money.cnn.com/2000/05/05/technology/loveyou/>.
- Koerner, Brendan I. "Inside the Cyberattack that Shocked the US Government." Wired. October 23, 2016. <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>.
- Kotkin, Joel and Mark Schill. "The Cities Creating the Most Tech Jobs 2017." Forbes. March 16, 2017. <https://www.forbes.com/sites/joelkotkin/2017/03/16/technology-jobs-2017-san-francisco-charlotte-detroit/#201597a38f6b>.
- Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum. February 26, 2013.
<http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.
- Laberis, Bill. "20 Eye-Opening Cybercrime Statistics." Security Intelligence. November 14, 2016. <https://securityintelligence.com/20-eye-opening-cybercrime-statistics/>.
- Library of Congress. "Articles of Confederation." Accessed November 4, 2017.
<https://memory.loc.gov/cgi-bin/ampage?collId=llsl&fileName=001/llsl001.db&recNum=127>.
- . "Judiciary Act of 1789." Accessed November 4, 2017.
<https://www.loc.gov/rr/program/bib/ourdocs/judiciary.html>.

- . “Thomas Jefferson: Establishing a Federal Republic.” Accessed November 4, 2017. <https://www.loc.gov/exhibits/jefferson/jefffed.html>.
- Lindsay, Bruce R. “Stafford Act Assistance and Acts of Terrorism.” Congressional Research Service. June 2, 2017. <https://fas.org/sgp/crs/homsec/R44801.pdf>.
- Liu, Edward C., Gina Stevens and Kathleen Ann Ruane. “Cybersecurity: Selected Legal Issues.” Congressional Research Service. April 17, 2013. <https://fas.org/sgp/crs/misc/R42409.pdf>.
- Madison, James. “Federalist Number 10.” Congressional Resources. 1787. <https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-10>.
- . “Federalist Number 44.” Congressional Resources. 1787. <https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-44>.
- . “Federalist Number 45.” Congressional Resources. 1787. <https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-45>.
- Malone, Scott. “Russian Election Hacking ‘Wildly Successful’ in Creating Discord: Former U.S. Lawmaker.” Reuters. May 4, 2017. <http://www.reuters.com/article/us-usa-trump-russia-idUSKBN17Y2ON>.
- Manfra, Jeanette. “Addressing Threats to Election Infrastructure.” Senate Intelligence Committee. June 21, 2017. <https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF>.
- Manuel Krogstad, Jens, Jeffrey S. Passel, and D’Vera Cohn. “5 Facts about Illegal Immigration in the U.S.” Pew Research Center. April 27, 2017. <http://www.pewresearch.org/fact-tank/2017/04/27/5-facts-about-illegal-immigration-in-the-u-s/>.
- Marr, Barnard. “Why Everyone Must Get Ready for the 4th Industrial Revolution.” Forbes. April 5, 2016. <https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/#a719f1e3f90b>.
- Maryland Department of Commerce. “IT and Cybersecurity in Maryland.” Accessed November 4, 2017. <https://open.commerce.maryland.gov/it-and-cybersecurity/>.
- Maura Healey. “Cyber Crime Strategic Plan.” Attorney General of Massachusetts. Accessed November 4, 2017. <http://www.mass.gov/ago/public-safety/cyber-crime-and-internet-safety/cyber-crime-initiative/strategic-plan.html>.

McCulloch v. Maryland. 17 U.S. 316. 1819.

Michigan. "Michigan Cyber Civilian Corps." Accessed November 4, 2017.
http://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html.

Michigan Department of Technology, Management and Budget. "Cyber Disruption Response Team." State of Michigan. October 2015.
http://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_Version_003_544764_7.pdf.

Miller, Mary Helen. "Data Theft: Top 5 Most Expensive Data Breaches." *The Christian Science Monitor*. May 4, 2011.
<http://www.csmonitor.com/Business/2011/0504/Data-theft-Top-5-most-expensive-data-breaches/3.-TJX-256-million-or-more>.

Mills, Elinor. "Melissa Virus Turns 10." CNET. March 31, 2009.
<https://www.cnet.com/news/melissa-virus-turns-10/>.

Morag, Nadav. "Federalism and Homeland Security: Our Constitutional System of Governance." Colorado Technical University. September 10, 2012.
<http://www.coloradotech.edu/resources/blogs/september-2012/federalism-and-homeland-security>.

Mosher, Dave and Skye Gould. "How Likely are Foreign Terrorists to Kill Americans? The Odds May Surprise You." *Business Insider*. January 31, 2017.
<http://www.businessinsider.com/death-risk-statistics-terrorism-disease-accidents-2017-1>.

Nakashima, Ellen. "Russia has Developed a Cyberweapon that can Disrupt Power Grids, According to New Research." *Washington Post*. June 12, 2017.
https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html?utm_term=.443461daea9c.

Naraine, Ryan. "Stuxnet Attackers Used 4 Windows Zero-day Exploits." ZD Net. September 14, 2010. <http://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/>.

NASDAQ. "7 Fastest-Growing Industries to Invest in for 2016." June 23, 2016.
<http://www.nasdaq.com/article/7-fastestgrowing-industries-to-invest-in-for-2016-cm639446>.

National Association of State Chief Information Officers. *2016 Deloitte-NASCIO Cybersecurity Study*. Accessed November 4, 2017.
<https://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf>.

- . “2016 NASCIO Award Nomination: Michigan Cyber Disruption Response Plan.” Accessed November 4, 2017. https://www.nascio.org/portals/0/awards/nominations2016/2016/2016MI9-Cybersecurity_Cyber%20Disruption%20Response%20Plan%20NASCIO.pdf.
- National Council of Information Sharing and Analysis Centers. “About ISACs.” Accessed November 4, 2017. <https://www.nationalisacs.org/about-isacs>.
- National Governors Association. “Act and Adjust: A Call to Action for Governors for Cybersecurity.” September 2013. https://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf.
- . “Gov. McAuliffe Named NGA Chair, Unveils Cyber Initiative.” July 16, 2016. <https://www.nga.org/cms/news/2016/gov-mcauliffe-cyber-initiative>.
- . “Governors O’Malley and Snyder to Lead NGA Resource Center on Cybersecurity.” October 2, 2012. https://www.nga.org/cms/home/news-room/news-releases/page_2012/col2-content/governors-omalley-and-snyder-to.html.
- . “Memo on State Cybersecurity Response Plans.” Accessed November 4, 2017. <https://ci.nga.org/files/live/sites/ci/files/1617/docs/MemoOnStateCybersecurityResponsePlans.pdf>.
- . “Resource Center for State Cybersecurity.” Accessed November 4, 2017. <https://www.nga.org/cms/center/issues/hcps/state-cybersecurity>.
- National Institute for Standards and Technology. “Cybersecurity Workforce Demand.” National Initiative for Cybersecurity Education. Accessed November 4, 2017. http://csrc.nist.gov/nice/NICE_Workforce_Demand.pdf.
- . “Framework for Improving Critical Infrastructure Cybersecurity.” February 12, 2014. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.
- National Security Act*, 50 U.S. Code 15 § 401.
- Naylor, Brian. “One Year After OPM Data Breach, What has Government Learned.” NPR. June 6, 2016. <http://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned>.

- Neil, Martha. "As State and Local Police Struggle to Investigate Cybercrime, Official Describes 'Helpless Feeling'." American Bar Association. April 21, 2014. http://www.abajournal.com/news/article/state_and_local_police_struggle_to_investigate_cybercrime/.
- New Jersey. "Mission." NJ Cybersecurity and Communications Integration Cell. Accessed November 4, 2017. <https://www.cyber.nj.gov/mission/>.
- New Mexico Department of Information Technology. "IT Strategic Planning." Accessed November 4, 2017. <http://www.doit.state.nm.us/strategicplanning.html>.
- New York City Mayor's Office of Tech and Innovation. "Building a Smart and Equitable City." Accessed November 4, 2017. <http://www1.nyc.gov/site/forward/innovations/smartnyc.page>.
- New York Daily News. "Here's How Trump's Plan to Defund Sanctuary Cities Could Play Out." November 23, 2016. <http://www.nydailynews.com/news/politics/trump-plan-defund-sanctuary-cities-play-article-1.2885423>.
- New York Times. "Headliners: Accessing Jail?" January 28, 1990. <http://www.nytimes.com/1990/01/28/weekinreview/headliners-accessing-jail.html>.
- New York v. United States*. 505 U.S. 144. 1992.
- Nivola, Pietro S. "Reflections on Homeland Security and American Federalism." Brookings Institute. May 13, 2002. <https://www.brookings.edu/articles/reflections-on-homeland-security-and-american-federalism/>.
- North Atlantic Treaty Organization. "Cyber Timeline." NATO Review Magazine. Accessed November 4, 2017. <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>.
- Nussbaum, Brian. "State and Local Cyber Security: The Rapid Growth of Cyber in Fusion Centers." Stanford University Center for Internet and Society. March 15, 2016. <http://cyberlaw.stanford.edu/blog/2016/03/state-and-local-cyber-security-rapid-growth-cyber-fusion-centers>.
- Obama, Barack. "Executive Order – Improving Critical Infrastructure Cybersecurity." White House Archives. February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

- . “Executive Order – Promoting Private Sector Cybersecurity Information Sharing.” White House Archives. February 13, 2015. <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.
- . “Presidential Policy Directive – Critical Infrastructure Security and Resilience.” White House Archives. February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
- . “Presidential Policy Directive – National Preparedness.” DHS. March 30, 2011. <https://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf>.
- . “Presidential Policy Directive – United States Cyber Incident Coordination.” White House Archives. July 26, 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
- Office of Legal Education Executive Office for United States Attorneys. “Prosecuting Computer Crimes.” Accessed November 4, 2017. <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>.
- Orbach, Barak, Kathleen S. Callahan, and Lisa M. Lindemenn. “Arming States’ Rights: Federalism, Private Lawmakers, and the Battering Ram Strategy.” *Arizona Law Review*. Vol 52. November 15, 2010. <https://ssrn.com/abstract=1696012>.
- Oregon Business Report. “Hacking a Problem for State Governments.” January 19, 2015. <http://oregonbusinessreport.com/2015/01/hacking-a-problem-for-state-governments/>.
- Pagliery, Jose. “Sniper Attack on California Power Grid May Have Been ‘an Insider,’ DHS Says.” CNN Technology. October 17, 2015. <http://money.cnn.com/2015/10/16/technology/sniper-power-grid/>.
- Perez, Evan. “U.S. Official Blames Russia for Power Grid Attack in Ukraine.” CNN Politics. February 11, 2016. <http://www.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/>.
- Peterson, Merrill D. *A Summary View of the Rights of British America*. Thomas Jefferson: Writings. New York: The Library of America. 1984.
- Polityuk, Pavel. “Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid.” Reuters. December 20, 2016. <http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF>.
- Printz v. United States*. 521 U.S. 898. 1997.

- Public Broadcasting Service. "A Short History of FEMA." November 22, 2005.
<http://www.pbs.org/wgbh/pages/frontline/storm/etc/femahist.html>.
- . "Birth of the Internet." Accessed November 4, 2017.
<http://www.pbs.org/transistor/background1/events/arpanet.html>.
- Radford University. "Gov. McAuliffe Announces Creation of Virginia Cyber Range." September 22, 2016.
<http://www.radford.edu/content/radfordcore/home/news/releases/2016/september/gov--mcauliffe-announces-creation-of-virginia-cyber-range.html>.
- Ridley, Gary. "Flint Hospital Confirms 'Cyber Attack,' Anonymous Threatens Action over Water Crisis." Michigan Live Media Group. January 22, 2016.
http://www.mlive.com/news/flint/index.ssf/2016/01/flint_hospital_confirms_cyber.html.
- Robbins, Gary. "USD Creating 'Cyber Range' to Train Students to Fight Digital Intruders." San Diego Union Tribune. October 6, 2016.
<http://www.sandiegouniontribune.com/news/science/sd-me-cyber-range-20161005-story.html>.
- Ross, Janell. "6 Big Things to Know about Sanctuary Cities." Washington Post. July 8, 2015. https://www.washingtonpost.com/news/the-fix/wp/2015/07/08/4-big-things-to-know-about-sanctuary-cities-and-illegal-immigration/?utm_term=.24508cc0b875.
- Sanchez, Gabriel. *Case Study: Critical Controls that Sony Should Have Implemented*. SANS Institute. June 1, 2015. <https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022>.
- Sanger, David E. "Obama Order Sped up Wave of Cyberattacks against Iran." New York Times. June 1, 2012.
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all.
- SANS Institute. "IDFAQ: What was the Melissa Virus and what can We Learn from it?" Accessed November 4, 2017. <https://www.sans.org/security-resources/idfaq/what-was-the-melissa-virus-and-what-can-we-learn-from-it/5/3>.
- Schmidt, Michael S. and David E. Sanger. "Russian Hackers Read Obama's Unclassified Emails, Officials Say." New York Times. April 25, 2015.
https://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html?_r=2.

- Schuman, Evan. *The TJX Data Loss and Security Breach Case*. University of Sydney: Engineering and Information Technology. 2007.
http://sydney.edu.au/engineering/it/courses/info5990/Supplements/Week07_Malware&Security/Supp07-4TJXCaseDetails.pdf.
- Serrano, Richard A. and Evan Halper. "Sophisticated but Low-tech Power Grid Attack Baffles Authorities." *Los Angeles Times*. February 11, 2014.
<http://www.latimes.com/nation/la-na-grid-attack-20140211-story.html#page=1>.
- Setalvad, Ariha. "Demand to Fill Cybersecurity Jobs Booming." *Stanford University Peninsula Press*. March 31, 2015.
<http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/>.
- Shelby County v. Holder*. 570 U.S. ___. 2013.
- Shueh, Jason. "For Funding, Colorado Cybersecurity Chief Says Strategy First." *State Scoop*. March 13, 2017. <http://statescoop.com/for-funding-colorado-cybersecurity-chief-says-strategy-first>.
- Siegel, Robert. "Pittsburgh Offers Driving Lessons for Uber's Autonomous Cars." *National Public Radio*. April 3, 2017.
<http://www.npr.org/sections/alltechconsidered/2017/04/03/522099560/pittsburgh-offers-driving-lessons-for-ubers-autonomous-cars>.
- Smith, Jason. "Digital Ballots, Outdated Machinery Leave Us Exposed to Russian Hack Round Two." *USA Today*. July 19, 2017.
<https://www.usatoday.com/story/opinion/2017/07/19/digital-ballots-outdated-machinery-leave-us-exposed-second-russian-hack-jason-smith-column/487825001/>.
- Somin, Ilya. "Federalism, the Constitution, and Sanctuary Cities." *Washington Post*. November 26, 2016. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/26/federalism-the-constitution-and-sanctuary-cities/?utm_term=.d8831a53e5da.
- Spidalieri, Francesca. *State of the States on Cybersecurity*. Pell Center for International Relations and Public Policy. 2015. <http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf>.
- Stanford University. "History of Stanford." Accessed November 4, 2017.
https://www.stanford.edu/about/history/history_ch3.html.
- . "What is Hacktivism?" Accessed November 4, 2017.
<https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html>.

- Symantec Corporation. “What is Cybercrime?” Accessed November 4, 2017.
<http://us.norton.com/cybercrime-definition>.
- Taylor, Harriet. “Metro Transport Systems Eyed after Hack Attack in San Francisco.”
 CNBC. November 28, 2016. <http://www.cnbc.com/2016/11/28/cybersecurity-experts-.html>.
- Texas Department of Information Resources. “2016-2020 State Strategic Plan for
 Information Resources Management.” Accessed November 4, 2017.
<http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/2016-2020%20State%20Strategic%20Plan%20for%20Information%20Resources.pdf>.
- The Federalist Papers Project. “Anti-Federalist Papers.” Accessed November 4, 2017.
<http://thefederalistpapers.org/anti-federalist-papers>.
- Totty, Michael. “The Rise of the Smart City.” Wall Street Journal. April 16, 2017.
<https://www.wsj.com/articles/the-rise-of-the-smart-city-1492395120>.
- Trump, Donald. “Presidential Executive Order on Strengthening the Cybersecurity of
 Federal Networks and Critical Infrastructure.” White House. May 11, 2017.
<https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.
- U.S. Constitution. amend. X.
- . art. I, § 8.
- . art. II.
- . art. III, § 1.
- . art. VI, § 2.
- United States Term Limits, Inc. v. Thornton*. 514 U.S. 779. 1995. (Kennedy, J.,
 concurring).
- Vaidya, Tavish. *2001-2013: Survey and Analysis of Major Cyberattacks*. Georgetown
 University. September 1, 2015. <https://arxiv.org/pdf/1507.06673.pdf>.
- Violent Crime Control and Law Enforcement Act*. 18 U.S. Code 211 § 3231.
- . 18 U.S. Code 227 § 3559.
- Virginia. “Cyber Veterans Initiative.” Cyber Virginia. Accessed November 4, 2017.
<http://cybervets.virginia.gov/>.

- . “Governor McAuliffe Announces \$1 Million in Cybersecurity Scholarships.” Accessed November 4, 2017.
<https://governor.virginia.gov/newsroom/newsarticle?articleId=16192>.
- Wallis, John and Wallace E. Oates. “The Impact of the New Deal on American Federalism.” National Bureau of Economic Research. January 1998.
http://www.colorado.edu/ibs/es/alston/econ8534/SectionX/Wallis_and_Oates,_The_Impact_of_the_New_Deal_on_American_Federalism.pdf.
- Ward, Mark. “A Decade on from the ILOVEYOU Bug.” BBC. May 4, 2010.
<http://www.bbc.com/news/10095957>.
- Ware v. Hylton*. 3 U.S. 199. 1796.
- Waxman, Seth P. “Federalism, Law Enforcement, and the Supremacy Clause: The Strange Case of Ruby Ridge.” *Georgetown Law Faculty Publications*. March 2010.
<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1279&context=facpub>.
- Weise, Elizabeth. “Yahoo Says 2013 Hack Hit All 3 Billion User Accounts, Triple Initial Estimates.” USA Today. October 3, 2017.
<https://www.usatoday.com/story/tech/2017/10/03/3-billion-yahoo-users-breached-company-says/729155001/>.
- White House. “Cyber Incident Severity Schema.” Accessed November 4, 2017.
<https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf>.
- . “Fact Sheet: Cybersecurity National Action Plan.” White House Archives. February 9, 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.
- . “The Constitution.” Our Government. Accessed November 4, 2017.
<https://www.whitehouse.gov/1600/constitution>.
- . “Thomas Jefferson.” Accessed November 4, 2017.
<https://www.whitehouse.gov/1600/presidents/thomasjefferson>.
- White, Sarah K. “Top U.S. Universities Failing at Cybersecurity Education.” CIO. April 25, 2016. <http://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html>.
- Wood, Colin. “Unmasking Hacktivism and Other High-Profile Cyberattacks.” Gov Tech. August 28, 2015. <http://www.govtech.com/public-safety/Unmasking-Hacktivism.html>.

- Yates, Robert. "Antifederalist Paper 45." The Federalist Papers Project. Accessed November 4, 2017. <http://thefederalistpapers.org/antifederalist-paper-45>.
- Zaleski, Andrew. "The Latest Hot Start-ups to Emerge from Israel's Cybersecurity War Machine." CNBC. February 28, 2017. <http://www.cnbc.com/2017/02/28/the-latest-hot-start-ups-to-emerge-from-israels-cybersecurity-war-machine.html>.
- Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired. November 3, 2014. <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.
- . "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired. March 3, 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
- Zinets, Natalia. "Ukraine Charges Russia with New Cyber Attacks on Infrastructure." Reuters. February 15, 2017. <http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN>.
- Zuckerman, Laura. "Montana Health Record Hackers Compromise 1.3 Million People." Reuters. June 24, 2014. <http://www.reuters.com/article/us-usa-hacker-montana-idUSKBN0F006I20140625>.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California